

Got Questions?



VERMONT COMPUTING INC.

Email us and we might feature your question in the newsletter!

newsletter@vermontcomputing.com

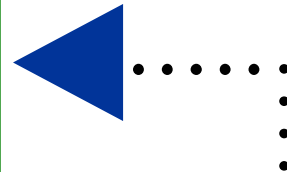


Store Hours

Mon – Fri 8:00 – 6:00

Sat & Sun 10:00 – 12:00

VCI



Vol 7 Issue 4 Feb. Part 2 Newsletter

IN THIS ISSUE:

VCI NEWS:

- *VCPC ADD-ONS, OFFICE 2007, FINGERPRINT READER*

TECH TIPS:

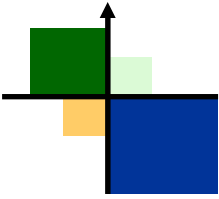
- *10 THINGS NOT TO DO TO YOUR COMPUTER*

PERIPHERALS:

- *DISK RELIABILITY*
- *ANTI-SPAM: NO PERFECT SOLUTION*
- *FIGHT DISEASE WITH GRID COMPUTING!*



Vermont Computing, Inc.
23 Merchants Row
Randolph, VT 05060
Tel: (802) 728-9217

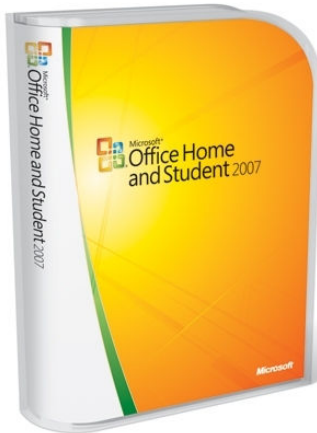


VERMONT COMPUTING, INC.

VCI NEWS

New Add-ons for Website "VC"PCs

Our current VCPCs, model .04 and 1.05 have gotten additional upgrade options. Conveniently configure your preferred PC on our website and let us build the new PC of your choice. Base prices starting at just \$399 and \$699 gives you room to add additional upgrades to suit your needs. Here is some of what's newly available:



Microsoft Office Home and Student 2007

Office Home and Student 2007 provides office software essentials to help you accomplish tasks more efficiently.

You can use Office Home and Student 2007 to create great-looking documents, spreadsheets, and presentations, and you can manage your notes and information in one place. With improved menus and tools, enhanced graphics and formatting capabilities, new information management tools, and more reliability and security, Office Home and Student 2007 makes working at home easier and more enjoyable.

Office Home and Student 2007 includes *Office Excel 2007*, *Office PowerPoint 2007*, *Office Word 2007*, and *Office OneNote 2007*.

Microsoft Fingerprint Reader

If you are like most people, you have more than a dozen passwords and user names to remember. Whether you are checking your e-mail for new messages, catching up on the news, posting to a Web discussion group, or playing games on the Web, you have to sign in all the time. Have you ever sat there, staring at your screen, wondering which password you set?

Wonder no more. Microsoft has developed a convenient solution for replacing all those passwords with something you do not have to worry about forgetting: your fingerprint. The Microsoft Fingerprint Reader lets you log on to your favorite Web sites without scrambling for passwords--just touch the fingerprint reader with a registered fingerprint whenever a password or user name is required, and you are in. Just like that.

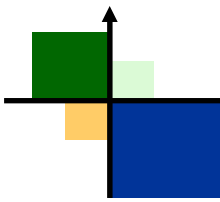


Many more! Check out our site www.vermontcomputing.com for more great products to compliment your purchase of a new PC.

Also new on the website, we have **VCI t-shirts and merchandise!** In association with CafePress, Vermont Computing is now offering fine Vermont Computing gear.

Proceeds will be donated to a **non-profit organization**.

Head on over to gear.vermontcomputing.com to pick up some VCI merchandise today.



10 dumb things users do that can mess up their computers

[Http://www.techrepublic.com/](http://www.techrepublic.com/)

Nervous newbies are often fearful that one wrong move might break the computer forever. Luckily, short of taking a sledge hammer to the box, the consequences aren't usually quite that dire. Even so, users often do create problems for their computers and for your network. Here's a description of common missteps you can share with your users to help them steer clear of preventable problems.

#1: Plug into the wall without surge protection

You may think your systems are in danger only during an electrical storm, but anything that interrupts the electrical circuit and then starts the current back again can fry your components...You can protect your systems against damage from power surges by always using a surge protector, but it's important to be aware that most cheap surge protectors will survive only a single surge and need to be replaced afterward. An Uninterruptible Power Supply (UPS)...has a battery that keeps power flowing smoothly even when there's an outage, to give you time to gracefully shut down.

#2: Surf the Internet without a firewall

Every Internet-connected computer should be protected by a firewall; this can be a firewall built into the broadband modem or router, a separate firewall appliance that sits between the modem/router and the computer, a server at the network's edge running firewall software, or personal firewall software installed on the computer (such as ICF/Windows Firewall built into Windows XP or a third-party firewall program like Kerio or ZoneAlarm).

#3: Neglect to run or update antivirus and anti-spyware programs

Let's face it: Antivirus programs can be a royal pain...But in today's environment, you can't afford to go without virus protection. The malicious programs that AV software detects--viruses, Trojans, worms, etc.--can not only wreak havoc on your system but can spread via your computer to the rest of the network. Spyware is another growing threat;...so it's important to run a dedicated spyware detection and removal program.

#4: Install and uninstall lots of programs, especially betas

The more programs you install, the more likely you are to run across ones that either include malicious code or that are poorly written and cause your system to behave improperly or crash. The risk is greater with pirated programs.

#5: Keep disks full and fragmented

One of the results of installing and uninstalling lots of programs (or adding and deleting data of any kind) is that it fragments your disk. Disk fragmentation occurs because of the way information is stored on the disk...You can use the disk defragmenter built into Windows (Programs | Accessories | System Tools) or a third-party defrag program to rearrange [the] pieces of files so that they're placed contiguously on the disk.

#6: Open all attachments

It used to be that you could assume plain text (.txt) or graphics (.gif, .jpg, .bmp) files were safe, but not anymore. File extensions can be spoofed; attackers take advantage of the Windows default setting that doesn't display common file extensions to name executables something like greatfile.jpg.exe. With the real extension hidden. You should open attachments only when they're from trusted sources and only when you're expecting them. Even if the mail with the attachment appears to come from someone you trust, it's possible that someone spoofed their address...

#7: Click on everything

Clicking on hyperlinks in e-mail messages or on Web pages can take you to Web sites that have embedded ActiveX controls or scripts that can perform all sorts of malicious activities, from wiping your hard disk to installing a backdoor program on your computer that a hacker can use to get in and take control of it...Think before you click a link. Links can also be disguised in phishing messages or on Web sites to appear to take you to a different site from the ones they really point to. For example, the link might say www.safesite.com, but it actually takes you to www.gotcha.com. You can often find out the real URL by hovering over the link without clicking it.

#8: Share and share alike

If you have file and printer sharing enabled, others can remotely connect to your computer and access your data. Even if you haven't created any shared folders, by default Windows systems have hidden "administrative" shares for the root of each drive. A savvy hacker may be able to use these shares to get in. One way to prevent that is to turn off file and printer sharing--if you don't need to make any of the files on your computer accessible across the network. If you do need to make shared folders accessible, it's important that they be protected by both share-level permissions and file-level (NTFS) permissions.

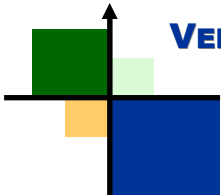
#9: Pick the wrong passwords

Don't pick passwords that are easy to guess, such as your birthdate, loved one's name, social security number, etc. Longer passwords are harder to crack, so make your password at least eight characters long; 14 is even better...Create a phrase you can remember easily and use the first letters of each word, along with logical numbers and symbols. For example: "My cat ate a mouse on the 5th day of June" becomes "Mc8amot5doJ."

#10: Ignore the need for a backup and recovery plan

Use the built-in Windows backup program (Ntbackup.exe in Windows NT, 2000, and XP) or a third-party backup program and schedule backups to occur automatically. Store backed up data on a network server or removable drive in a location away from the computer itself, in case of a natural disaster like flood, fire, or tornado.

Visit <http://www.techrepublic.com/> for the full article.



PERIPHERALS

Google Releases Paper on Disk Reliability

<http://www.slashdot.org/>

"The Google engineers just published a paper on Failure Trends in a Large Disk Drive Population. Based on a study of 100,000 disk drives over 5 years they find some interesting stuff. To quote from the abstract: 'Our analysis identifies several parameters from the drive's self monitoring facility (SMART) that correlate highly with failures. Despite this high correlation, we conclude that models based on SMART parameters alone are unlikely to be useful for predicting individual drive failures. Surprisingly, we found that temperature and activity levels were much less correlated with drive failures than previously reported.'"

5 Things the Boss Should Know About Spam Fighting

<http://www.slashdot.org/>

"Sysadmins and email administrators were asked to identify the one thing they wish the CIO understood about their efforts to fight spam. The CIO website is now running their five most important tips, in an effort to educate the corporate brass. Recommendations are mostly along the lines of informing corporate management; letting bosses know that there is no 'silver bullet', and that the battle will never really end. There's also a suggestion to educate on technical matters, bringing executives into the loop on terms like SMTP and POP. Their first recommendation, though, is to make sure no mail is lost. 'This is a risk management practice, and you need to decide where you want to put your risk. Would you rather risk getting spam with lower risk of losing/delaying messages you actually wanted to get, or would you rather risk losing/delaying legitimate messages with lower risk of spam? You can't have both, no matter how loudly you scream.'"

Grid Computes 420 Years Worth of Data in 4 Months

<http://www.slashdot.org/>

Da Massive writes with a ComputerWorld article about a grid computing approach to the malaria disease. By running the problem across 5,000 computer for a total of four months, the WISDOM project analyzed some 80,000 drug compounds every hour. The search for new drug compounds is normally a time-intensive process, but the grid approach did the work of 420 years of computation in just 16 weeks. Individuals in over 25 countries participated.

" All computers ran open source grid software, gLite, which allowed them to access central grid storage elements which were installed on Linux machines located in several countries worldwide. Besides being collected and saved in storage elements, data was also analyzed separately with meaningful results stored in a relational database. The database was installed on a separate Linux machine, to allow scientists to more easily analyze and select useful compounds."