

News from Campus
Technologies, January 2009



Welcome back, everyone! We hope you had a good break and came back refreshed and renewed and ready to hit the ground running for the spring term. While we try to turn out a newsletter monthly during the fall and spring terms, we have not had the time to get a newsletter out since the end of October! We've simply been too busy keeping everything running to gather articles and put together the *News*. We'll try to catch you up on the highlights in this issue.

Self Help Portal now available: CT has developed a Self Help Portal to assist users with technology-related questions. Access <http://ct.mansfield.edu/self-help/> for demos, FAQs, PowerPoint presentations, printer documentation and more. Also available on this site are links to password reset interfaces. For employees, **if your Active Directory password has expired**, did you know that you can still log in to the [Employee Active Directory Password Change](#) interface with your old password and change it? **If you have forgotten your password**, you can also access the [Employee Active Directory Password Self-Help](#) and reset your password. (You will be required to enter your email address, your ID number and the last four digits of your ssn).

FrontPage is being retired: At the end of the Spring 09 semester, Microsoft FrontPage software will be retired! It is past the end of its lifecycle and is no longer supported by Microsoft. If anyone is still using FrontPage to edit webpages, please email Suzanne Murphy – smurphy@mansfield.edu. We will be providing training on Dreamweaver during the spring semester for any faculty/staff who currently use FrontPage to maintain their websites.

VCRs on the way out: If you haven't noticed, VCRs are getting harder to find. Actually the latest tape units are found combined with DVD players and are just players, not recorders. And frankly, VCP quality is way down, since the assumption is being made that video tape is an obsolete technology headed for the dumpster. It's been out of the mainstream for several years now and the writing IS on the wall: CT will not be able to maintain support for video tapes indefinitely. This is the time to consider how you will transition from video tape to an alternative media. While budgets are thin, the cost of copying an existing video tape or the portions of the tape you use for your classes to DVD is practically nil. Our AV group headed up by Mark Polonia can discuss your needs and help you plan for the transition. Make no mistake about it; video tape is going the way of the 16mm movie projector as a classroom tool. Consider yourselves warned! Our next announcement will likely be a drop-dead date for general support of video cassettes in classrooms. Start planning for this transition now!

Budget woes interrupt replacement cycle: For several years the CT group did its best to replace campus desktop computers in a regular, scheduled cycle. Our goal was a 3-year cycle, but the realities of our budgets generally stretched the cycle out to four years and sometimes five. We've been receiving a lot of questions lately..."when will MY desktop computer be replaced?" Unfortunately, CT has not been funded for continuing a regular replacement schedule at this time. We are using our budgeted funds to provide upgrades and replacement machines where need is most critical. Our intent is to fund upgrades as-necessary to keep desktop computers operational, but we may have to wait out the current economic downturn before we can get back into a regular planned replacement cycle again.

As for "Vista" – Not now, not soon. Just as we jumped over Windows 2000 and went directly to XP, expect us to bypass Vista in favor of Windows 7, due out later this year. It will take us a while to completely cycle out all the desktop computers that are

inadequate to properly run a new flavor of Windows, so again, a lot depends on our future budgets.

Concerns over Cart System ‘Alterations’: CT reviews all our classrooms prior to each semester startup to verify all the equipment we support is fully functional. We also take feedback received from the campus community and usage information from the systems themselves to direct our maintenance efforts where they are needed most. Ensuring our classroom technology is functional remains one of our highest priorities. There are common issues with our cart systems we need your help with. Here are some of problems we find:

- Carts used as storage medium: We commonly find glasses, articles of clothing and all manner of paperwork on the classroom carts. Often times, paperwork is left on top of the sound systems, blocking airflow and creating a fire hazard at worst, and shortening the life of the components at best.
- Modified Carts: We often find cart systems have been re-wired in interesting ways. Whether someone decided to “borrow” a piece of equipment, then returned it knowing not how to actually reinstall it, or someone trying to work around a perceived problem we can’t say. We can say that we find cart systems dead or damaged by *creative rewiring*. The cart system PC’s are altered by installing unsupported software, personal files are downloaded to the PC, and operating system functions are changed to non-standard settings – video cards reset from our standard to either very low or very high resolutions are common. This makes the cart far less friendly for the next user, if they find they can use it at all.
- Missing remote controls, extension cords and other electronics: Probably the most common call we receive is when a faculty person notes a remote control is missing. Those of us who are charged with keeping the carts operational often shake our heads in wonder – first, what

happens to those remotes, and second, where are WE going to find yet another replacement remote control for a piece of equipment that is no longer manufactured? Second most popular missing item: gyromice and gyromouse receivers. The latest gyromouse sports a receiver that looks like a thumb drive... Sadly, they are NOT thumb drives, they are a whole lot more expensive, and they disappear with disappointing regularity. As for extension cords... they're available from the store room or Wal-Mart cheap, but apparently, not cheap enough for some. But on the bright side, losing the extension cord actually prevents the next problem, which is:

- Carts moved further than their umbilical cords allow: We often find wiring covers cracked, loosened or broken, end caps popped off or entire sections of wiremold pulled loose from the wall after someone decides a cart with a 6-foot umbilical cord needs to be 6 feet 1 inch from the wall.

CT will offer any group or individual training on any or all aspects of our cart systems. We are also in the process of rewriting cart usage instructions and placing them on the web, though it stands to reason these instructions won't help much if the cart system can't be brought on line! Each cart should have with it a document to assist in troubleshooting. To ensure everyone has the best experience possible when using the classroom technology carts, CT would again ask you to help US help YOU by following these simple do's and don'ts:

- DO note any anomalies in operation and report even minor problems to the CT HELP desk at your first opportunity. Be as specific as possible so the technical staff can repair the problem in one trip. Many of our rooms are scheduled so tightly that multiple classes may be inconvenienced by a problem, and our opportunities to make repairs are limited.
- DON'T alter the cart system in any manner! Altering the cart to accommodate your personal tastes may have unintended consequences for the next user, even making

the system unusable! If you feel you must change something, consider why that is necessary – perhaps you should make a case for changing our standard. And most certainly, if you change something – CHANGE IT BACK to our standard before leaving the room!

- DO return the remotes to the cart when your class is concluded and ensure gym mice are returned to their chargers.
- DO make certain all students have left the room and the doors are locked prior to leaving.
- DON'T load software on the cart computers or use the computer desktop, or cart top, as your personal storage space or filing cabinet!
- DO take care in moving the cart. Stay comfortably within the umbilical cords range, move the cart slowly and ensure the umbilical does not get tangled.
- DO have, if at all possible, a “Plan-B” in the event of technical problems.

Personal computer backups: CT has been asked about how often we back up staffer's personal computers. Or... calls come in where it's clear that the end-user assumes CT is keeping backups of user's computers. So here's the scoop: CT does NOT back up end-user computers! We back up files when someone gets a replacement PC so we can restore them to their new one, but these backups are only kept for a short span of time – a month or two at most. It has always been CT's perspective – relayed repeatedly over the years – that the end user must take responsibility for housekeeping their computers and backing up critical data. We don't see that changing any time soon.

So... end users! If you don't know how to back up your critical files, contact the help desk to schedule training time. All university computers have CD/DVD writers that can make short

work of saving your data. With blanks costing only pennies the time it takes to create backups is the real cost. And what value do you place on peace of mind?

Of course, this discussion begs the next question: Just how does one determine what is critical to be saved? If you're like many of us, you never do ANY data housekeeping and so your PC contains every memo, document and E-mail you've sent and received over the last 15 years! We encourage you to review your files to determine just what you actually need to keep. By housekeeping your data you'll find that backups take only a fraction of the time and space needed otherwise plus it ensures that you actually have a handle on what you're saving and where it is!


Just as it is necessary to go through your files at home to review, re-arrange, toss and cross-reference every once in a while, your PC requires the same treatment. There's no time like when you back up your critical files to do a bit of housekeeping to ensure you can find important documents if and when you need them. If you need help coming up with a plan for cleaning up and backing up your critical data, give the Help desk a call. We'll point you in the right direction!

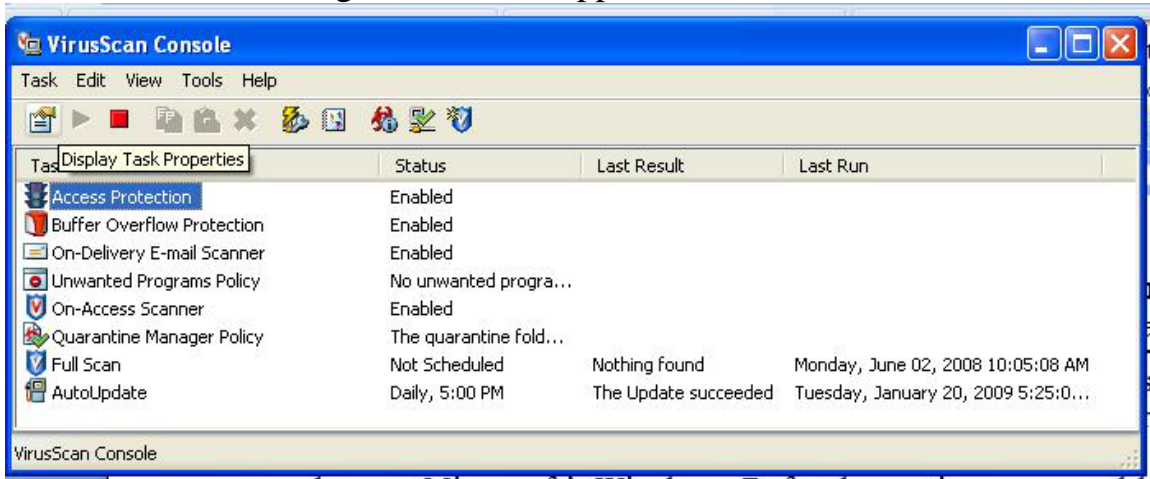
Tools being added to our spyware/malware arsenal:

It's getting worse all the time; Folks shipping out spyware and malware are doing their best to stay one step ahead of those of us charged with keeping them out of our network and your PC. CT is adding additional software to lock out spyware and malware. Microsoft's Windows Defender anti-spyware add-on will soon be pushed out as a general campus application. To help minimize the impact on your day, times of automatic scans will be adjusted to make the scanning process less intrusive.

How to Avoid Spyware: There are several things you can do to ensure your computer remains "clean" and free of spyware and malware. First, the defenses:

Antivirus products MUST be kept up-to-date: McAfee antivirus is a fully-featured and solid product, available to all University staff and students as a free download from the My.Mansfield site. It is our first line of defense, so it's a good idea to check every so often to be certain it is updating properly and full scans are being run.

To check McAfee: First, locate the McAfee shield in the Notification Area of your task bar. The shield looks like this: . By right-clicking the shield, you will be presented with several options. By choosing "VirusScan Console" the following window will appear:

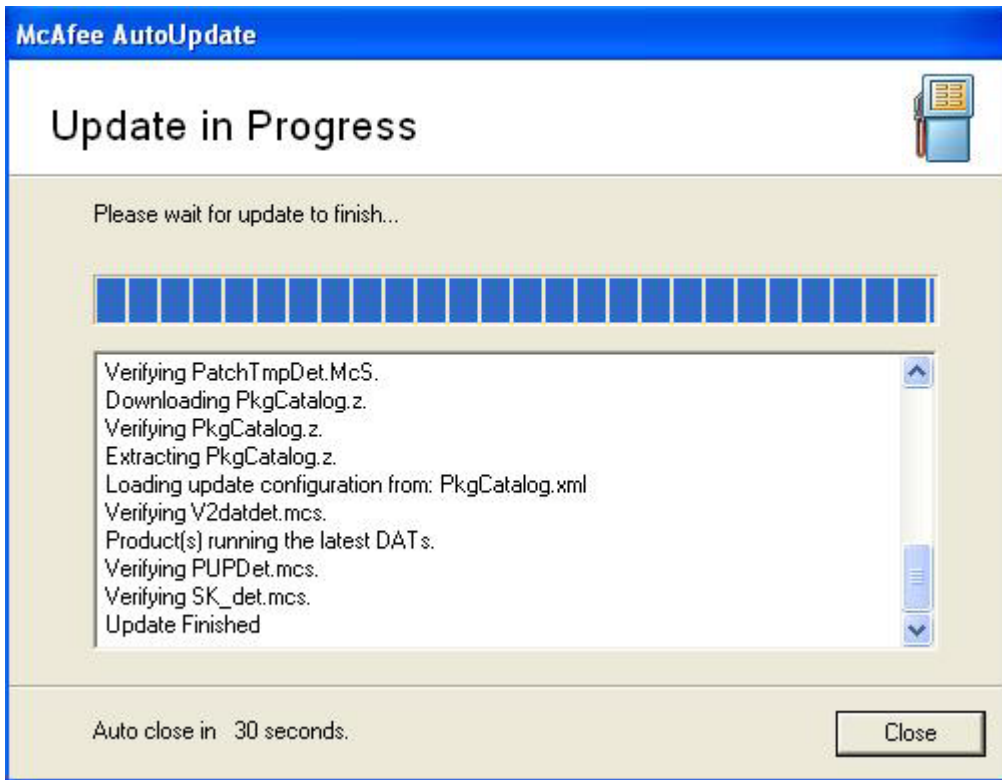


Your console window should look similar, with the On-Access Scanner Enabled and Access, Buffer, and On-Delivery E-mail protection **Enabled**. You will also see the last time an AutoUpdate was attempted and if it succeeded. If that date is more than a week old, you should manually perform an update. And if you're like this user and haven't run a full scan on your computer in a while (next-to-last entry), it's probably time you did.

OK, so now you know what's-what with McAfee. If your AutoUpdate is not working, let's begin a manual update – it only takes a few minutes.

--Close the Console screen.

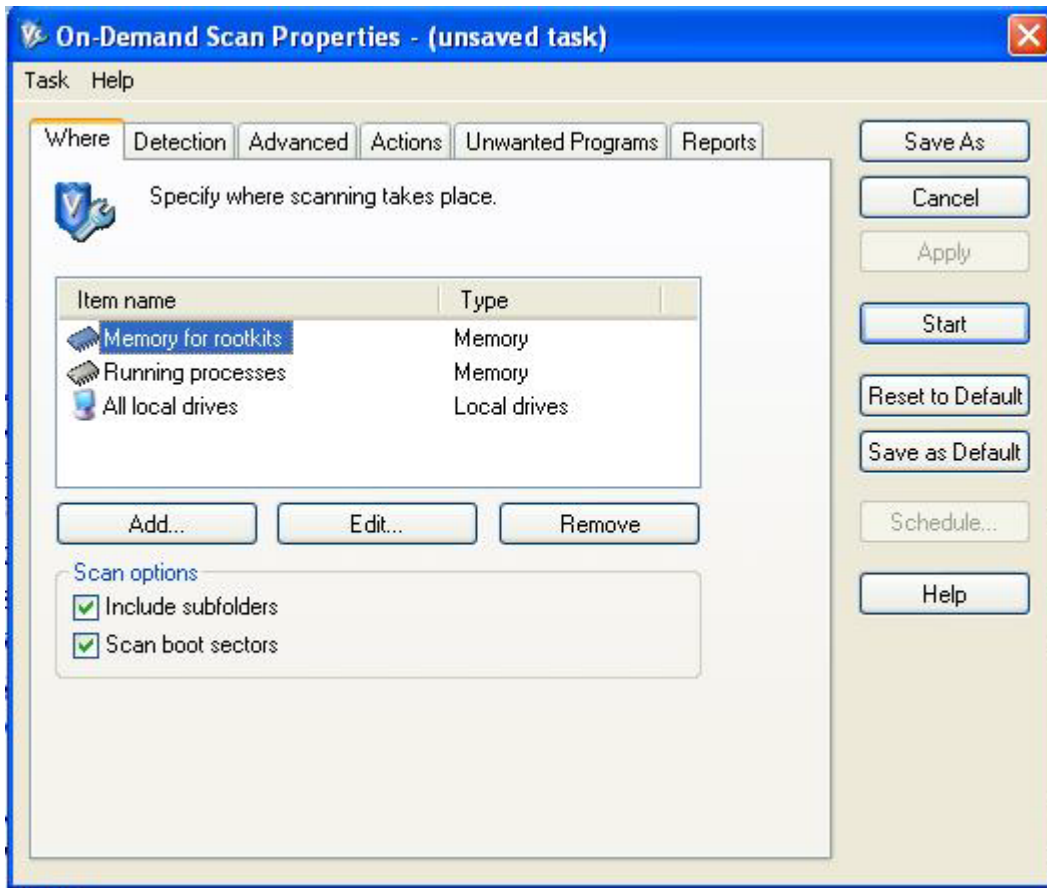
--Right-click on the McAfee Shield again, and this time choose "Update Now". You'll see a screen similar to this one:



If you'll note the third line from the bottom, you are advised "Product(s) running the latest DATs.". That is what we hope to see at the end of the process. If you see information indicating that new files are being downloaded, then allow the process to complete – it may take a few additional minutes, but it does ensure you are running the latest-and-greatest. It's also important that, if new files are being downloaded, at the end of the process you see a message saying "the Update Succeeded". If in doubt, go back to the VirusScan Console and verify a successful update there.

If you find that McAfee is not auto-updating on your university computer, advise the Help desk so we are aware and can check your system settings further.

Running a full system scan should be done at least a few times a year – more often if you are inclined to download "stuff" from the Internet. Simply right-click on the shield, then choose "On-Demand Scan". You'll see the following window appear:



Default values will scan all your local disks as well as the computer's memory and running processes – simply press the “start” button to begin. This process may take a several **hours** to complete and if you perform the scan during working hours it **WILL** slow your machine. It may be advisable to allow the scan to run over a period when you are not going to need the computer, such as an evening or a period of the day when your computer use is less intense.

Firewall services: At the present time we rely on the university's firewall to keep users free of many of the ills that plague the Internet. We are in the process of adding sophisticated exemption files and Policies to university computers so the Windows Firewall will work properly in our complex environment. As for your HOME computer, It's always a good idea to run a firewall product. Since most of us would rather let the computer do most of its own heavy lifting, the firewall present in Windows XP and beyond is a good choice for the casual user. You may discover that, after enabling the firewall, you have problems with some types of products running. A quick check on the Internet usually shows you a work-around, but do BE

CAREFUL if a web site tells you simply to exempt them from firewall checks. This is typical of sites that deliver Trojan Horses to your computer! Check with us or some other person savvy about such things before risking opening holes in your firewall that are best left closed!

The more computer-savvy home users may wish to try ZoneAlarm. Checkpoint software's most basic firewall is a free product that can be configured to advise you when it intercepts suspected bad stuff heading in *either* direction, and asks you whether you should allow or deny the movement of data to or from the Internet this one time, or every time.

Beware Peer-to-Peer file-sharing services: Yep, just because you found a great piece of audio or video on the Internet doesn't mean the next package you grab may be everything you expected. NEVER download executables via Peer-to-Peer networks as this is the best way to lose control of your PC to the evil empire! Sophisticated malware can disable your antivirus software – you may receive a warning and it appears that your antivirus product is still there protecting your computer, but it has, in fact, been compromised. We recommend downloading executables only from vendors you trust.

Beware your Email! Do NOT open Email flagged (SpamTag) if you don't know what it is. NEVER open Emails or attachments from unknown persons. We try to warn everyone when Phishing attacks are in-progress, but of course this means the attack is already underway! Remember: We will NEVER ask you to reply to any message with personal information! Nor will your bank, your credit card company, or other legitimate vendor! If you have concerns about the legitimacy of an Email, contact the company directly via a known, advertised Email address or phone number.

Rogue Installs: Never install products you don't need. Often products we don't want are tagged onto products we do want, often by the most reputable companies. For example, when you install Adobe Acrobat, if you don't watch carefully and uncheck a box you'll also receive the Yahoo! Toolbar. That's not bad if you need another tool bar, but other sites will tell you – if you read the fine print – that they will “from time to time extract data on your computer usage”. And even though what they're doing is legal and no directly identifiable personal information is transmitted, a lot can be extrapolated about your life, your computer use, and your surfing habits. Less than scrupulous organizations could install such things as keystroke

loggers and other monitoring software without your knowledge or consent! Even purchased software may install small-footprint products designed to “phone home” from time-to-time. They say they only check for updates, but do they? What other data may tag along? For that reason, it’s a good idea to read that legalize that’s in the EULA – End User License Agreement. Again, a quick check of the ‘web often will show you hazards a quick read-through may miss.

Have your computer checked: Occasionally in spite of our best efforts, “stuff” sneaks through. If your computer is suddenly far more sluggish than it’s been, it’s probably a good time to check to see what all is running in the background. While not necessarily bad in and of themselves, each little gadget and gadget added to your machine takes cycles and acts to slow down normal operation. Some interfere with each other. And some gadgets ARE Trojan horses – software offering you a handy tool while providing its designer access to your machine. Evaluating running processes is beyond what we can teach you here, but it IS a good idea to let us know if your university computer is suddenly running slower than normal with no new software installed. We can review the running processes to ensure nothing untoward or unnecessary is using up cycles. Home users should call their computer repair guru to have a look-see. Before ending or blocking a process, it’s always a good idea to back up your system critical files using Microsoft’s System Restore utility.

What about Macs? Because the Mac still does not enjoy a great penetration into the enterprise and in total holds a very small percentage of the computer market, the number of occurrences of malware and spyware remain only a fraction of what plagues the PC. That said, every type of malware exists for the Mac and other unix variants: viruses, Trojans, key loggers, spyware – you name it. And as important, did you know the Mac can spread PC malware without being affected itself? So while we do not yet have a university-supported Mac solution, we do strongly encourage Mac users to educate themselves and purchase appropriate antivirus products.

* * * * *

That’s about it for this month. As always, contact the Help desk if you have any questions or would like more information about any of the topics we’ve covered here. Also, if you would like to see a particular issue discussed in a future issue of the *News*, let us know. We’re here to help!