



# IT UPDATE

November 2005

## Storing Your Data Files

Network drives are available to faculty and staff with varying levels of security. IT recommends users, whether Mac or PC, to store data on a network drive rather than their local (C:) drive. Network drives include:

- H:** is for departmental data, which is accessible to everyone in your department. Subdirectories with further restrictions can be created for administrators or secretaries for all departmental-related files.
- O:** is your private directory. No other user has access to it. This is for information that would not be needed if you were to leave the university.
- W:** is a campus-wide shared directory. This drive is for sharing files with faculty and staff.
- S:** is for faculty to share course-related files with students
- M:** is for students to store their files

### Why store your files on a network drive instead of your local drive?

#### You could lose your files today!

Since January of this year, we have experienced sixteen drive failures on desktop computers. Will the next one be yours? Without warning you could lose all of your files stored on your local (c:) drive.

#### Viruses and worms may require an emergency rebuild.

Depending on the type of virus, an emergency rebuild may be required. Your files could be at risk of being corrupted or deleted. Backing up and restoring your files will prolong your downtime.

#### You can access your network drives in the classroom.

Your O:drive is automatically mapped when you log in to the computer in the classroom or lab.

#### You can access your network drives from home.

Simple instructions are available for PCs and for Macs on our Web page,. Visit [www.iusb.edu/~sbit](http://www.iusb.edu/~sbit) and select "Internet, Phone, and Video Connections."

#### Rebuilds and upgrades would be quicker.

When files are stored on network resources, you don't need to spend hours backing up and restoring your files to your local (c:) drive. (See article in lower right corner of this page.)

#### Network drives offer more security and are backed up daily.

Multiple layers of redundancy and security protect data stored on network drives from loss due to server drive failure. In addition, backups which are maintained for three months, provide recovery in cases of extreme disaster.

## CFS storage space to be discontinued

If you currently use Filemanager in the original Oncourse or Common File System (CFS), you are encouraged to move your files to your Oncourse CL Resources area or other file storage media during the fall semester. **Both CFS and the original Oncourse Filemanager will be retired following the spring 2006 semester. CFS will be read-only as of January 2006.**

In addition to the larger storage capacity per user (250MB) offered in Oncourse CL, it also has its own Resources area for instructors to post course resources. Find out more about using Oncourse CL Resources by clicking "Training & Support" on the Oncourse login page, <http://oncourse.iu.edu/>.

## Do you know where your files are?

If you aren't sure where your files are being saved or don't understand the concept of drives, directories and subdirectories, you may want to consider taking the "File Management" class from Continuing Education. IT will fund this class and other computer application classes for staff and faculty. For instructions to register for a class, visit the IT home page, [www.iusb.edu/~sbit](http://www.iusb.edu/~sbit) and select "Training and Workshops."

## More Wireless Coverage

IT staff are working to increase wireless access on campus. The first phase which provided wireless access in all of the student gathering places was completed last year. Coverage has now been updated to include most offices and classrooms in Wiekamp and Northside Hall, and further enhancements are expected. Wireless access is to supplement, not replace, hardwired access.



## You are responsible for backing up files on your local drive

Since network storage is provided, users are now responsible for backing up and restoring any files they keep on their local c:drive, when IT has to rebuild or replace their computer.

IT strongly recommends taking advantage of the benefits of storing important files on the network drive (H: or O:).

# What you should know about the dangers of the Internet

Computers have become very useful tools for communications, banking, shopping, entertainment, staying in touch with friends and family and learning about any number of interesting topics. However, the Internet has a dark side and most people are completely unaware of the pitfalls which come with this fascinating online world.

Among the malicious intentions of those who would compromise your computer are: to gain access to your personal data for identity theft, to use your computer to send spam, or be used to attack other computers on the network, to use your computer to "hack" other computers or simply as the act of juvenile mischief to wreak havoc.

Whatever the intent, you owe it to yourself to understand the dangers and learn how to protect yourself as it may save you countless headaches and in some cases, a substantial amount of money.

LET THE WEB SURFER BEWARE!!



## Securing your home computer and laptop

So you just bought a computer brand new, took it out of the box, set it up and have begun surfing the web. You may be thinking that since the computer is new, it should have all the software and safety precautions built in already. Well, you're probably wrong.

Whether you have an older computer or a brand new one, there are steps you need to take to ensure the security of your system. IU South Bend IT does not support users' home equipment or personal equipment brought on campus. However, we strongly recommend you take a few precautions to protect yourself. The information provided in this section is simply a guide and is provided for your benefit.

The first thing that you need to know is that Windows 95/98 and Windows ME are not secure operating systems when connected to the Internet. IU South Bend IT strongly recommends that if you are on the Internet with a Windows based computer, use Windows XP with Service Pack 2 (SP2) and keep the software updated.

While it is true that Mac OS or Linux based computers are not as frequently targeted by viruses and hackers, there are vulnerabilities and viruses written specifically for those operating systems as well and it is important to keep these operating systems patched with the same vigilance as a Windows based user.

## Security at your IU South Bend workstation

- At IU South Bend, each workstation setup by IT has Symantec Antivirus software installed which is centrally updated. However, some viruses actually disable the update and protective features of anti-virus software. Ensure that Symantec Anti-virus is being kept up to date via Live Update and is performing regularly scheduled scans. – [ <http://kb.iu.edu/data/agzb.html> ]. When you initially start Symantec Antivirus, the date of the Virus Definition File should rarely be more than a week old.
- Lock your workstation when it's not in use ("Windows Key – L") or log out. Never leave your workstation unattended while logged in.
- Update Spybot [ <http://kb.iu.edu/data/anfq.html> ] and scan your office computer at least once a week, [ <http://kb.iu.edu/data/angd.html> ].
- Update Adaware [ <http://kb.iu.edu/data/anfa.html> ] and scan your office computer at least once a week [ <http://kb.iu.edu/data/alrm.html> ].
- Never keep a database or list of individuals' personal information on computers other than those designated by IT as database servers.
- Inform IT if you bring up a server on campus and follow the IT Server Security Guideline.
- **Never share your password with anyone at any time** . This includes family, friends, fellow workers, and IT staff.
- It is ILLEGAL to share music and other media files if you do not have appropriate permission to distribute the files. Check the options you have set in file-sharing programs like Morpheus, KaZaA, Aimster, and Gnutella. To read more about Indiana University 's policy on file sharing, see <http://filesharing.iu.edu/>.
- Never give out personal information (such as your Social Security #) via e-mail or on an insecure Web page, or if you are concerned that your information might be intercepted and used illegally.
- Clear your Web browsers cache periodically, or set the cache to expire at regular intervals. For details, visit [ <http://kb.iu.edu/data/abts.html> ]

## Likely ways to get spyware and viruses

### First and foremost understand three things:

1. Trust no message sent to your computer from anyone.
2. Free is not free.
3. Visiting websites which are unknown to you is dangerous.

The three most common ways computers become infected is from opening email attachments which contain malware, downloading files off of the Internet or visiting a malicious website.

Many worms use email to send spam and to spread themselves to other computers. They use email addresses that are found in email address books on the infected computer so that the email appears to come from people you know. These emails are disguised as something official or useful such as security updates for your computer or official business from a bank or IT department. Never trust emails with links to security updates. Be aware that emails which appear to come from people you know may contain harmful links. These links are usually disguised as innocent Web locations.

Another very common way of catching a virus is from downloading things from the Internet. The most common websites are those that offer free downloads such as screensavers, background images, pornography, music files or any other free download you can imagine. Internet scoundrels have even figured out a way to put viruses in pictures that you can download and save to your computer. Another very common way of getting malware infections is use of P2P software such as Kazaa or Morpheus. Again, free is not free.

The third most common way to end up with an infected computer is by simply visiting websites setup to lure visitors with the intent of tricking the user in to clicking on a link which will download malicious software. You may be offered free software or images, or a pop up window may appear which will download malware whether you click 'OK' or 'Cancel' or 'Exit' or any other button, or you may be tricked in to clicking on a link to a page which actually downloads malware. Internet Explorer is the most targeted web browser which is why IU South Bend IT recommends alternative web browsers such as Firefox from Mozilla.org.

Now for a fact which may surprise you. You can turn on your computer, have it attached to the network, not be reading email, not surfing the web, not downloading anything, and be vulnerable, simply by being attached to the network. It has been documented that an unprotected, unpatched computer attached to the network may be compromised in as little as eight minutes.



To find these articles and more information regarding security on the internet visit the Information Technology home page and select Internet Security.

## Beware of scams on the Internet relating to phone service!

**Cramming** occurs when charges or services (voice mail, Internet access, etc.) are added to an account without authorization by the customer. Recently, employees of IU South Bend have unwittingly signed up for unwanted services! If you sign up for a service unintentionally, you may be exposing yourself or your department to unwanted phone charges!

### Tips to avoid cramming

- Always read the fine print before completing a contest or sweepstakes form. This is particularly important when completing a form on the Web (the fine print may be very fine). Offers for "free" coupons usually have strings attached. This is the single, biggest cause of cramming – contests, sweepstakes and offers with fine print, such as coupons.
- Be careful when calling unfamiliar 800 numbers. You may unwittingly sign up for a service.
- Always review your monthly phone bill for unfamiliar charges.

## IT Helpdesk

DW1245

Hours:

8:00 am—8:30 pm, Mon-Thurs.

8:00 am—5:00 pm, Friday

[www.iusb.edu/~sbit](http://www.iusb.edu/~sbit)

Phone: 574-520-5555

E-mail: [helpdesk@iusb.edu](mailto:helpdesk@iusb.edu)

# Classroom Technology Support

## ***New Location***

Classroom Technology Support (CTS) has relocated from Northside to their remodeled digs in Wiekamp 1145. CTS staff are responsible for the installed technology in all generally-scheduled classrooms. This includes the tech desks, computers, DVD/VCR players, projectors, overheads, and document cameras. The staff are available to resolve your classroom problems, listen to your suggestions for classroom enhancements, and provide instruction in the use of technology.



*Meet the staff and enjoy some refreshments to celebrate our new location 3 - 5 p.m. on Wednesday, November 9th, 2005.*

## ***Reporting Problems***

Phones have been placed in the technology classrooms so that you can quickly contact CTS. Just dial the help line, 5555, and press "1" for classroom technology support.

In some cases we can resolve your problem over the phone by talking you through the resolution. In other cases we may be able to manipulate equipment centrally to resolve the issue. If needed, we can send a technician to your classroom or deliver replacement equipment.

## ***Classroom Upgrades Planned***

Plans are underway this semester to upgrade the old tech desks so that all classroom technology on campus will be operated in the same way. We hope to be doing some of these installs yet this semester, so please bear with us during the process.

Rooms being upgraded include Northside 036, 104, 106, 108, 125, 152, Greenlawn 102, 104, Riverside 107, and Wiekamp 1135, 1175, 1275, and 1290.

We will also be installing technology in four generally-scheduled seminar rooms in Wiekamp: 2170, 2260, 3160, and 3260.

The following rooms pose cabling and room design challenges, but are on schedule to receive installed equipment by July 2006 : Northside 013, 113, 071, 0063 and DW1001.

## ***Need a Document Camera?***

If your classroom doesn't have a document camera but you would like to use one this fall 2005 semester, please let us know. Please contact CTS in person at DW1145 or call x5555 and press "1".

## **Two New Members on the IT/User Support Team**

**Tiernan Armstrong-Ingram** joined CTS in April of this year as the technology consultant. He has an Associates degree in Philosophy from IU South Bend, and is completing his BA in Philosophy with a minor in Informatics. He had previously worked for us part-time on the Helpdesk.

**Brian Emmons** joined the Helpdesk staff in September. He has a BS in Computer Technology from Purdue University and has several years of user support experience. Both members have greatly enhanced our User Support and are pictured below .



CTS staff pictured above (from left), Tiernan Armstrong-Ingram, Jessie Onderdonk, and Manager Kathleen Weidner



Helpdesk staff pictured above (from left), Manager Mike Fletcher, Andrew Evans, Brian Emmons, Hoy Henry III, and Andrew Walton