Avoid the worry...

STAY SECURE

Information Technology Services
University of Illinois at Springfield
**STEP 1**

**STAY SECRET**

Protect Your Passwords

Your NetID allows you to safely access numerous resources at UIS, including your personal email account. Protecting your password helps keep your personal information out of the hands of cybercriminals.

**About your Password:**
- Make it complex: It must contain at least one uppercase letter, one lowercase letter, and one digit. It cannot contain any common word or proper name and cannot be less than 8 characters.
- Never write it down anywhere. Memorize it.
- Keep it to yourself. Do not disclose it to anyone.
- Change it at least once a year.
- Visit http://www.uis.edu/its/netid/ for more info

**Q & A**

"This campus is supposed to be wireless! Why can’t I connect to the internet with my laptop?"

A wireless connection to the internet requires use of the VPN. This ensures that a secure, encrypted connection is made without the risk of unauthorized use. The VPN installer can be downloaded free of charge at the UIS websote (http://webstore.uis.edu).

**Did You Know?** Every residential UIS student is required to sign a campus computing and network acceptable use policy. If you have not signed this you might lose your network access. To obtain a copy that you can sign, contact ITS Support at 206-6000.

**STEP 2**

**STAY LEGAL**

Avoid the Risk

Information Technology Services at UIS is committed to the protection of creative thoughts and works in the academic community. In the same regard, ITS upholds the standards set by the Digital Millennium Copyright Act that seek to protect the creative authors of copyrighted material. The basis of this act is simple; if you don’t own it, you can’t download it. This includes movies, music, and software that are protected by legal copyright.

While programs like LimeWire, BearShare, KaZaA, and eMule are not illegal themselves, it is against the law to use them for downloading movies and songs that you do not own. The Recording Industry Association of America is currently fighting legal battles against colleges across the nation to make sure this point is known. They are suing universities to hand over the personal information of users that illegally download music. The end result: the information is released and the students themselves are sued. So far there is only one way to guarantee that this does not happen to you: do not download or distribute music and movies that you do not own. Otherwise, instead of searching for that hot new MP3, you may be searching for a lawyer.

**Q & A**

"Windows wants me to use a firewall. Won’t that help?"

While Windows Firewall can be useful, it can interfere with some parts of the campus network. UIS requires that you turn off the Windows Firewall to connect to the campus network. Luckily, UIS has its own firewalls that will keep an eye on who is connecting to your computer. If you are off-campus and surfing the web from a different source (Panera, Starbucks, parents home, etc.) then you should temporarily turn Windows Firewall back on.

**STEP 3**

**STAY PROTECTED**

Avoid Viruses

The moment your computer connects to the internet it becomes susceptible to virus attacks. The campus network has firewalls to help protect your computer, but no tool is completely effective. McAfee VirusScan Enterprise adds a significant additional level of protection and is required to be installed on all faculty, staff, and student computers that are to be connected to the UIS Network. Best of all, it’s FREE to download from the UIS websote.

**Know the facts and stay protected:**
- McAfee VirusScan Enterprise is available at http://webstore.uis.edu
- If your computer came with “free antivirus software,” it is probably only a trial edition and will do little to protect your computer from new viruses.
- Since your computer must have McAfee VirusScan, it is best to uninstall all other virus protection software from your computer. This will prevent them from conflicting with McAfee VirusScan and slowing down your computer.
- Mac users should use Virex, (also available free from the webstore)

**Q & A**

"My computer came with free antivirus software when I bought it! Isn’t that enough?"

Even though you computer came with free antivirus software, the updates for the software are not free. Having antivirus software installed is not enough, it must be continuously updated to protect against new viruses. McAfee Antivirus is available to install and update free of charge to all UIS students, staff, and faculty.
STEP 4

STAY PRIVATE

Smash the Spyware

Spyware not only slows down your computer it also secretly steals your personal information for strangers to see. Unfortunately, installing and running antivirus software is not enough to keep hackers from looking at your hard drive. Using simple and FREE programs such as Spybot and AdAware can help keep others out of your computer.

Get Smashing: Download and use at least one of the following:

- Spybot-Search and Destroy
  Available at http://www.safer-networking.org

- Adaware
  Available at http://www.lavasoftusa.com

- For more information, visit
  http://www.uis.edu/its/techsupport/spyware.html

Q & A

“My computer is slower than molasses! What’s going on?”

Even the most casual surfing and downloading can make your computer home to various breeds of spyware. This not only puts your information at risk, it also bogs down your computer. Luckily, free programs such as AdAware and Spybot can help you get your privacy and your speed back.

Did You Know? Programs such as McAfee VirusScan, AdAware, Spybot, and the VPN can be installed from a free CD available at the UIS helpdesk. To obtain a copy of this CD go to the Help Desk on the first floor of HSB and request a “UIS Housing CD.”

STEP 5

STAY SMART

Safe Habits = Safe Computer

Staying well informed and making good decisions is your best tool for protecting your computer. Make sure you know what you are doing when it comes to downloading files. If you are not sure what the file is or where it is coming from, chances are it’s a trap. Do you use blogs, forums, Myspace, Facebook, etc.? Use extreme caution when giving out or posting contact information. Even a simple e-mail address posted on a blog can become the target of junk mail harvesting.

Steps to keep you smart:

- Do not install or use Peer-to-Peer applications such as Limewire, Gnutella, eMule, Morpheus, etc.

- Do not respond to ANY email message that asks for personal information. This is almost certainly a phishing scam to steal your identity. Remember, if an email looks fishy, it’s probably phishing.

- Never accept suspicious file transfers or open suspicious IM messages or email messages

- Always use the VPN when connecting from off-campus (visit http://www.uis.edu/its/techsupport/vpn.html for more info)

- Avoid problems. Contact Tech Support Center with your questions (206-6000).