

Conditions of Access

All computers that connect to the campus network must meet the Conditions of Access:

1. The computer must have the university-approved version of McAfee VirusScan or Virex installed and updated. If you have another anti-virus product installed, you must remove it and install the university-approved version.
2. The computer must have all available security updates installed. This includes all security updates for the host operating system, as well as available security updates for installed software.

Any computer that fails to comply with the Conditions of Access may be taken offline until it can be updated so it meets the requirements.

Why have conditions for access?

Internet threats reduce your ability to use your computer for academic pursuits, research, and public service.

Viruses cause major problems.

In a short time, a single infected computer can infect many other unprotected computers, which can lead to network interruptions or failure.

Protect against Denial of Service (DoS) attacks.

Vulnerable computers can be used by hackers and viruses to launch attacks that deny everyone access to important servers and services.

Security is everyone's responsibility.

You need to do your part to keep the campus network safe for yourself and others.

More Information

To get more information about security and the campus network, please refer to the following resources.

University Computer Help Desk

Julian Hall 115 309.438.HELP
www.helpdesk.ilstu.edu

TechZone

Bone Student Center 206 309.438.8334
www.techzone.ilstu.org

ResNet

www.resnet.ilstu.edu

Telecommunications & Networking

www.telecomm.ilstu.edu

Appropriate Use Policy

www.policy.ilstu.edu/fiscal/appropriate_use_policy.htm

Outages & Alerts

www.ilstu.edu/alerts

ULID Password Change and Self-Reset

www.ilstu.edu/ulid

Microsoft Windows Updates

windowsupdate.microsoft.com
(External Site)

Mac OS X Updates

www.apple.com/support
(External Site)

Federal Trade Commission — Identity Theft

www.consumer.gov/idtheft/
(External Site)

Security is Everyone's Responsibility.

Get Secure.
Stay Secure.

are YOU???
secure???



“I work hard to make the Internet dangerous.”

—ANONYMOUS HACKER

I would introduce myself, but I prefer to remain anonymous. I can assure you that I work hard to make the Internet dangerous. Follow my advice, and you'll be making my job easier.

Please run your computer without anti-virus software. Most of the emails I send have viruses, and anti-virus software makes it hard to infect you.

Hand over your personal info too. I'll take your social security number, credit card numbers, passwords, and anything else you'd like to give me. I'll use your info to apply for credit cards and loans, which will probably ruin your credit rating (not that I care).

In case you're leery about submitting your personal info online, I've set up a website and made it easy for you. I designed the site to look like eBay so you'll feel safe. If you don't use eBay, I have more to choose from, so take your pick—you might even find one that looks like your bank's website.

I have other websites too. Just search for “screensavers” or “free music” to find them. Some hijack your web browser, and the others give you annoying spyware. You don't mind if I use your computer to send spam, do you? Thanks a bunch.

Are you a member of MySpace or FaceBook? That's outstanding. I recommend you post every incriminating picture of yourself and every personal detail for the world to see. When billions of people have access to that kind of information, what could go wrong?

Lots of people on the Internet want to help you out—people like me.

The Internet is teeming with dangerous people like this. Use the strategies in this brochure to protect yourself.

What we do for you

Illinois State University is dedicated to making sure you and your data stay safe.

We are serious about viruses.

Anti-virus software is free – Download McAfee VirusScan and/or Virex. Both are provided to you at no cost.

VirusScan stays updated – Centrally-managed computers on ResNet and in campus offices get updates automatically.

Email is scanned – Before email arrives in your Inbox, it's scanned. Infected email and the worst spam are blocked.



The network is safe and reliable.

The network is protected – The campus network is guarded against dangerous computers on the Internet.

The network is safe – Campus computers must meet the Conditions of Access, which means they are up-to-date.

VPN and wireless are secure – VPN from off campus and wireless on campus are encrypted, secure connections.

How you can protect yourself

For all its benefits, the Internet poses many dangers as well.

Be skeptical.

If it sounds too good (or terrible) to be true, it could be a fake. Don't blindly trust websites, emails, or instant messages—they could be trying to trick you into doing something you will regret.

Think before you click.

Don't just click links without thinking first. Who sent you the link? Do you trust that person? If you are asked to “verify your information” online, it could be a phishing scam.

Know your anti-virus & anti-spyware.

You should know how to use your anti-virus and anti-spyware programs like McAfee VirusScan and Ad-Aware. Scan your computer for spyware and viruses regularly to keep it healthy.

Don't flaunt your MySpace.

When you join sites like MySpace and FaceBook, use discretion. The personal info and pictures you put online may come back to haunt you.

Avoid risky searches.

Your search results may contain links to dangerous websites, especially if you use search terms like “free screensavers” or “download music”.

