

IT Security Practices

While Departmental and Campus IT units are accountable for the security of computer networks; computer and data security is also each individual's responsibility. In addition, researchers are often responsible for the management of research data that may fall under privacy policies and standards and/or require a formal privacy and data security plan.

Please work with your IT units to make sure that your personal computers, the computers you are using or managing on campus, as well as the data they contain are secured at all times. An unprotected computer is especially vulnerable to cyber attacks, spam, or other threats that can compromise a user's identity or undermine the security of a computer's hardware and data. Even before you connect to Internet either in or outside the campus, make sure that your computer will be as safe as possible from viruses and other malicious programs that are rampant on the Internet.

Listed below are some general recommendations and best practices for ensuring the security of data on your machines.

Best Practices

1. Patch and Critical Updates

Make sure that your machines (Windows, Mac, Linux or any OS) are up-to-date with latest patches for Operating system and installed software. [Learn More](#)

2. Install Anti-virus/Anti-spyware software

Every machine should have Anti-virus threat protection software installed on it. The anti-virus software should be constantly updated with new virus definitions. Most anti-virus software today are bundled with anti-spyware, firewall and other protections as well. [Learn More](#)

3. Choose strong password

Be as creative as possible while choosing a password. Choose strong passwords with letters, numbers, and special characters to create a mental image or an acronym that is easy for you to

remember – but not anyone else. Do not use the same password for all important accounts and change passwords regularly. [Learn More](#)

4. Protect sensitive data

Make sure that the data on your laptops, USB drives and other mobile devices is encrypted. This will help prevent unauthorized access to your sensitive data in case your mobile device is stolen. There are several good software available for encryption purposes. TrueCrypt is one of the best free open-source disk encryption software.

Securely remove sensitive data files from your hard drive, which is also recommended when recycling or repurposing your computer. You can also purchase USB flash drives with strong encryption. [Learn More](#)

5. Backup

Backing up your machine regularly can protect you from the unexpected. Keep a few months' worth of backups and make sure the files can be retrieved if needed. [Learn More](#)

6. Control Access to your machine

Don't leave your computer in an unsecured area, or unattended and logged on, especially in public places. The physical security of your machine is just as important as its technical security. [Learn More](#)

7. Use email & internet safely

Ignore unsolicited emails, and be wary of attachments, links and forms in emails that come from people you don't know, or which seem like an obvious phishing attempt to access your personal data. Avoid downloading from unknown and untrustworthy sites. [Learn More](#)

8. Use secure connections

When connected to the Internet, your data can be vulnerable while in transit. Use remote connectivity and secure file transfer options when off campus. [Learn More](#)

9. Use desktop firewalls

Windows and Mac computers have basic firewalls built in which could provide additional security and protect your computers from unwanted visitors. [Learn More](#)

Recommendations

Patch

If your local IT staff allows, set machine for automatic updates. If not, please try to restart your machine for latest updates when you see the 'yellow shield' (Windows machine) on the right side of the taskbar or when you get message that 'updates are ready to be installed on your machine'.

Install Protective Software

University of Illinois provides all of its faculty, staff and students threat protection software for free. If you've administrative privileges on your machine, make sure these programs are installed. If not, please check with your local IT department for assistance.

[University of Illinois WebStore](#)

Chose Strong Password

Do Choose

- Something **easy for you (but not anyone else) to remember** with at least eight characters. Longer the password, stronger it is.
- Use numbers, special characters and capital letters in your password. Replace alphabets with numbers or special characters where possible. For e.g. 'Mount Everest' can be converted to 'M0unt3v3r35t'.
- Create passwords out of phrases, favorite quotes, songs, TV Shows etc. by abbreviating, spelling backward, using numbers and special characters.
- Here are some more tips on choosing s strong password:

<http://www.microsoft.com/protect/fraud/passwords/create.aspx>

Do not choose

- Dictionary words, your name, name of friends, close relatives etc. – not even spelled backwards or with special character.
- Your userid or userid spelled backwards.
- Passwords of fewer than at least six characters.
- A previously used password or a password used for more than one account.
- Phone numbers, birthdays, anniversary dates etc.
- All alphabets or all numeral passwords.

Protect Sensitive Data

TrueCrypt is just one example of good free encryption software.

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

If you choose to, you can also buy advanced encrypted flash drives that are encrypted with multiple levels.

<http://www.ironkey.com/enterprise>

Backup

Your local IT support might already be backing up your emails and few folders. However, you can also back up of important folders on frequent basis to maintain redundancy. You can either use your personal USB flash drives or USB hard drives OR you can use Tivoli Storage Manager client to backup data on ACCC servers.

<http://www.uic.edu/depts/accc/software/adsmnew/intro.html>

Control access to your machine

Always lock your machine even when you might be going away only for a few minutes. A software-based theft recovery program like 'LoJack for laptops' might be useful to track, recover and/or delete data remotely in case your laptop gets lost or stolen.

<http://www.absolute.com/products/lojackforlaptops>

Use email and Internet safely

Never open spam emails. Please verify authenticity of the website before entering any personal information.

Use secure connections

Please ask your local IT support to assist you with setting up secure VPN or remote connections to your campus machine from your laptop or home machine if you want to work remotely.

Use Desktop Firewalls

In addition to these local firewalls, it is recommended to have a 3rd party firewall installed on your machine. Usually, anti-virus suites come with these in-built firewalls. Please contact your local IT department for more help with firewall settings.