INDIANA UNIVERSITY

Best practices for computer security

Important:

As of June 18, 2016, Symantec no longer provides antivirus updates for its Endpoint Protection product. To help keep your computer protected against viruses f you have Endpoint Protection installed, uninstall it and instead use one of the antivirus applications UITS recommends.

This document details how you can secure your computer, accounts, and the data stored on them. Information Security Best Practices contains more technical security precautions that you should know, and that IT Pros should implement.

All information in this document applies to laptops, but for further details, see Laptop Security.

For help, contact your campus Support Center.

Note:

Following some of the suggestions below can affect how your computer interacts with the network. If your computer or local network is managed by a computer support provider, you should consult with your provider before making changes to avoid disrupting your network connection.

On this page:

    - Do not download unfamiliar software off the Internet
    - Do not propagate virus hoaxes or chain mail
    - Log out of or lock your computer
    - Shut down lab/test computers
    - Remove unnecessary programs or services
    - Restrict remote access
    - Treat sensitive data very carefully
    - Remove data securely
    - Deploy encryption whenever it is available
- Securing your home network

Top four things you can do to protect your computer

Use security software

- The most important thing you can do to keep your computer safe is to install and maintain security software.

  > **Note:**
  >
  > For recommendations about antivirus software, see Recommended antivirus software at IU.

- Install and run Identity Finder, a tool to help you search for, protect, and dispose of personal information stored on your computer, file shares, or external media.

- Install the Secunia Personal Software Inspector. This will alert you when your current software applications are out of date or require a security update.

Practice the principle of least privilege (PoLP)

Practice the principle of least privilege. Do not log into a computer with administrator rights unless you must do so to perform specific tasks. Running your computer as an administrator (or as a Power User in Windows) leaves your computer vulnerable to security risks and exploits. Simply visiting an unfamiliar Internet site with these high-privilege accounts can cause extreme damage to your computer, such as reformatting your hard drive, deleting all your files, and creating a new user account with administrative access. When you do need to perform tasks as an administrator, always follow secure procedures. For more, see Account Privileges.

Maintain current software and updates

Use a secure, supported operating system; see ComputerGuide: Deals by vendor, recommendations, and common questions. Keep your software updated by applying the latest service packs and patches. Refer to your operating system's help for assistance.

The best way to maintain third-party software is to install the Secunia Personal Software Inspector. This will alert you when your current software applications are out of date or require a security update.

Frequently back up important documents and files

Back up your data frequently. This protects your data in the event of an operating system crash, hardware failure, or virus attack. UITS recommends saving files in multiple places using two different forms of media (e.g., Cloud Storage or USB flash drive). See At IU, what options do I have for storing files?

Avoid threats to your computer

- **Never share passwords or passphrases:** Pick strong passwords and passphrases, and keep them private. Never share your passwords or passphrases, even with friends, family, or computer support personnel.

  Note:

  At Indiana University, no official communication (e.g., email message, phone call, or computer support consultation) will ever include a request for your Network ID passphrase.

  For more, see:

  - About your IU passphrase
  - May I allow someone else to use my IU computing account?
  - At IU, how can I see my login activity?
  - If I give my passphrase to someone else who uses my account to send a harassing email message, will I be held responsible?

- **Do not click random links:** Do not click any link that you can't verify. To avoid viruses spread via email or instant messaging (IM), think before you click; if you receive a message out of the blue, with nothing more than a link and/or general text, do not click it. If you doubt its validity, ask for more information from the sender.

- **Beware of email or attachments from unknown people, or with a strange subject line:** Never open an attachment you weren't expecting, and if you do not know the sender of an attachment, delete the message without reading it. To open an attachment, first save it to your computer and then scan it with your antivirus software; check the program's help documentation for instructions.

- **Do not download unfamiliar software off the Internet:** KaZaA, Bonzi, Gator, HotBar, WhenUSave, CommentCursor, WebHancer, LimeWire, and other Gnutella programs all appear to have useful and legitimate functions. However, most of this software is (or contains) spyware, which will damage your operating system installation, waste resources, generate pop-up ads, and report your personal information back to the company that provides the software.

  Obtain public domain software from reputable sources, and then check the newly downloaded software thoroughly, using reputable virus detection software on a locked disk, for signs of infection before copying it to a hard disk.

  Note:

  Before you choose to download and use these types of programs, make sure you are not violating copyright or other applicable laws. Downloading or distributing whole copies of copyrighted material for personal use or entertainment without explicit permission from the copyright owner is against the law. For more, see:

    - File Sharing & Copyright from Protect IU
    - What happens if I receive a copyright infringement notice, and how can I avoid it?
    - What is the Digital Millennium Copyright Act?

- **Do not propagate virus hoaxes or chain mail:** For more, see:
  - What should I know to avoid getting in trouble with email?
  - How can I tell if a computer virus alert is a hoax?

- **Log out of or lock your computer when stepping away, even for a moment:** Forgetting to log out poses a security risk with any computer that is accessible to other people (including computers in public facilities, offices, and shared housing), because it leaves your account open to abuse. Someone could sit down at that computer and continue working from your account, doing damage to your files, retrieving personal information, or using your account to perform malicious actions. To avoid misuse by others, remember to log out of or lock your computer whenever you leave it.

- **Shut down laboratory or test computers after you are finished with them:** For computers in the UITS Student Technology Centers (STCs) or Residential Technology Centers (RTCs), logging out is sufficient to protect the security of your accounts and data. With other computers, however, it is usually necessary to shut them down after you have finished to prevent unauthorized access. Shutting down a computer prevents others from hacking it remotely, among other risks.
- **Remove unnecessary programs or services from your computer:** Uninstall any software and services you do not need.
- **Restrict remote access:** UITS recommends that you disable file and print sharing. In rare exceptions when you may need to share a resource with others, you should format your drive using NTFS, and correctly set the file and directory permissions.

  UITS also recommends disabling Remote Desktop (RDP) and Remote Assistance, unless you require these features. If you do, enable the remote connections when needed, and disable them when you're finished. Note that you only need to enable RDP on the computer you intend to connect to; disabling RDP on the computer you're connecting from will not prevent you from making a connection to another computer.
- **Treat sensitive data very carefully:** For example, when creating files, avoid keying the files to Social Security numbers, and don't gather any more information on people than is absolutely necessary.

  At IU, sensitive information should be handled (i.e., collected, manipulated, stored, or shared) according to legal and university functional requirements related to the specific use involved, as well as data and security policies of the university; see Protecting Data. For more, contact the university Data Steward for the data subject area involved; see the Committee of Data Stewards.
- **Remove data securely:** Remove files or data you no longer need to prevent unauthorized access to them. Merely deleting sensitive material is not sufficient, as it does not actually remove the data from your system. For information on secure data removal, see Secure Data Removal.
- **Deploy encryption whenever it is available:** For more, see:
  - What are secure websites and SSL/TLS certificates?
  - At IU, what is PGP Whole Disk Encryption (WDE)?

Securing your home network

For advice on securing your home network, see How can I secure my home wireless network?

Back to top

Related documents

- How can I protect data on my mobile device?
- At IU, how do I report a suspected information or information technology (IT) security issue?
- If I use social networking sites such as MySpace or Facebook, how can I protect my personal information?
- How can I be sure that a website is genuine?

This is document akln *in the Knowledge Base.*
Last modified on 2016-07-08 00:00:00*.*