phishing
Don’t be a phishing scam victim. Reputable organizations will never ask for personal data, account numbers, or passwords via email. Visit kb.iu.edu/data/arf8.html for more info.

copyright
Get the facts on downloading & sharing free &/or copyrighted material. It’s your job to ensure you’re downloading and sharing legally. Visit filessharing.iu.edu for more info.

protect your information
Your info is valuable! You work hard to build credit — protect your personal info online. Always think twice before releasing your name, address, phone, credit card, or SSN.

security software
Install anti-virus and anti-spyware software. Update them and the operating system regularly — most software will remind you, and you can even schedule the updates overnight for convenience.

firewalls
A firewall is your computer’s first line of defense. Most operating systems like Windows, Mac OS, and Linux have built-in firewalls, but may not be turned on by default — ensure you enable it.

keepITsafe.iu.edu
1. Don’t open files from strangers — and ensure that files from friends are legitimate. They could otherwise contain viruses or malware.

2. Consider the Principle of Least Privilege. Restrict your everyday computing account from having administrative privileges — this significantly reduces the risk of system damage by viruses and malware.

3. Never give personal info online to someone you don’t know — including your name, email, phone numbers, addresses, photos, or your Social Security Number.

4. Use strong passwords; include combinations of lower and uppercase letters, numbers, and symbols. The longer your password, the better. Consider a passphrase — a short phrase or favorite song lyric.

5. Never respond to SPAM or phishing; it only validates your email address. Set up filters to block SPAM and learn to recognize phishing attacks.

6. When your computer prompts, be sure to update your operating system and anti-virus software. Doing this regularly will give your computer the latest security updates and keep it from getting viruses.

7. Always back up your data — you never know.

8. Know exactly how parental controls work — and what they can and can’t do.

9. Know your wireless network, and use VPN as often as possible when using public Wi-Fi. Unencrypted data can be unknowingly “sniffed” through the air — a common practice for identity thieves.

10. Contact the 24x7 UITS Support Center with questions.
    online: uits.iu.edu
    email: ithelp@iu.edu
    chat: https://ithelp.iu.edu
    phone: 812-855-6789 / 317-274-4357