

Security Best Practices

Install **anti-virus software** on your University systems.

Choose **“hard-to-guess” passwords** for the applications and systems you access.

Apply **patches and updates** to University systems you use or manage on a frequent and consistent basis.

Use **screen-saver locks** or shut down your system when you are away for extended time periods.

A special thanks to Georgia State University for their assistance!

WSU – CaTS Computer Security

Patricia Vendt

Wright State University

040 Library Annex

937/775.4035

<http://www.wright.edu/security>

Information Security Awareness



**WRIGHT STATE
UNIVERSITY**

***Protecting Client
Information from Harm***

Guidelines for WSU
Employees & Students

Did you know a single compromised system on your campus can...

- Allow someone to steal SSNs and sensitive information
- Result in identity theft, crimes, and fraud
- Give someone access to accounts and/or passwords
- Expose sensitive or confidential information
- Cause your internet and e-mail access to be halted
- Attack other systems over the Internet
- Cause your computer to be compromised!

A single "unaware" University computer user can...

- Open a virus attachment in an e-mail and unknowingly infect unprotected systems on campus
- Implement file sharing and as a result, allow anyone over the Internet to see and delete the entire contents of their C: drives.
- Give someone access to accounts and/or passwords
- Expose sensitive or confidential information
- Cause your internet and e-mail access to be halted
- Attack other systems over the Internet
- Cause your computer to be compromised!

WSU Guidelines

1. Keep viruses off your computer! Install anti-virus software and scan your files regularly. Never click on e-mailed links or attachments from strangers.
2. Back-up financial/sensitive data to your network directory, not to your computer's hard drive. Encrypt these files to keep unauthorized persons from accessing this information and don't leave printouts sitting around. Do not save protected data to a removable storage device, phone, or PDA.
3. Use hard-to-guess passwords for all of your university accounts. Use a pass phrase that you can remember with a mixture of lowercase and uppercase letters, numbers, and symbols.
4. If you have a computer that you use to access the campus network remotely, install a personal firewall to add another important layer of security and connect over the Virtual Private Network (VPN).
5. Don't attach an external modem to your campus system and leave it set on auto answer.
6. Never comply with requests for personal information from an e-mail or phone call unless you initiated the contact.
7. Update and apply patches to your university systems on a regular and consistent basis. Microsoft issues new security patches often and if you fail to install them, your system can become vulnerable to attacks and intrusions. UNIX and Mac users must be vigilant in installing necessary patches as well.
8. Don't expose your accounts and passwords by writing them on notes that are stuck on your desk or computer monitor.
9. If you are going to be away from your computer for extended periods of time, turn on a password-protected screensaver, log off the network, lock your workstation, or shut your system down.
10. Lock rooms and file cabinets where paper records are kept.
11. Encrypt sensitive customer information when it is transmitted electronically over networks or stored online.
12. Recognize fraudulent attempts to obtain customer information.
13. Keep customer information secure and confidential. Report any suspected instances of fraud or negligence to your supervisor!

<http://www.wright.edu/security>