

Free Tools

There are a number of free tools available to assist you in maintaining a clean computer.

Student Computer Clean-Up

The Help Desk maintains a student computer clean-up page where you will find information on the recommended free anti-virus programs and spyware/malware removal tools. This information is located at:

webster.edu/helpdesk/restech/

THESE TOOLS ARE NOT TO BE INSTALLED ON WEBSTER OWNED COMPUTERS!

Online Virus Scan:

House call

<http://housecall.trendmicro.com>

PopUp Blocker:

Panicware Popup Stopper

http://www.panicware.com/product_psfree.html

Spyware Detection and Removal:

Ad-Aware

<http://www.lavasoftusa.com/support/download>

Please note: This software is suggested, but is not supported on campus. You will have to contact the software site or company for any support and questions for these products.

Other Helpful Links

- For additional information on *spyware/adware* or *viruses* visit:
www.webster.edu/depts/acs/virus.html
- For additional information on *internet security* visit:
www.webster.edu/helpdesk/tips.html

Webster University
Informational Brochure Series

Internet Security



Webster
UNIVERSITY

WORLDWIDE

Help Desk

support@webster.edu
www.webster.edu/helpdesk
866-435-7270 • 314-968-5995

Spyware, Adware & Malware

What is Spyware?

- Spyware is computer software that gathers and reports information about you without your knowledge or consent.

What is Adware?

- Adware or advertising-supported software is any software application in which advertisements are displayed while the program is running. These applications include additional code that displays ads in pop-up windows or through a bar that appears on a computer screen.

What is Malware?

- Malware is software that is intended to damage or disable a computer system; short for malicious software. Viruses are an example of malware.

How does Spyware/Adware/Malware get on my computer?

- Simply browsing the internet can cause spyware/adware to be picked up on your machine. Sometimes they arrive as an automatic download from a website or they may be embedded in the installation of a free or illegal piece of software. Opening email attachments can also put spyware on your machine.

How can I protect my computer from Spyware/Adware?

- Be judicious in what websites you choose to view and frequent. The viewing of websites with questionable content may install malicious spyware/adware on your machine without your knowledge.
- Do not utilize file sharing services. Often times the software associated with these services utilizes spyware/adware.
- Do not click on pop up ads while viewing internet sites.

- Be judicious in your software download practices. Certain free shareware programs contain “adbots” and other spyware/adware software.

How can I protect my computer from Malware?

- Do not open any attachments unless you are positive they are legitimate
- Do not download any files from the internet unless it is from a trusted, secure site
- If you suspect you have a virus, call the Help Desk immediately. Do not attempt to delete a virus on your own.
- Keep an updated anti-virus software package on your machine

Good Internet Security

Millions of people browse the internet everyday creating the potential for the security of your personal identity or your computer to be at risk. The best way to avoid these risks are by following these simple guidelines.

Online Purchases/Financial Transactions

- Check the privacy statement of the website that you are using to ensure that they cannot sell/rent your information without your consent.
- Ensure that you read and fully understand the policies of the website before you make any purchases. If you have any questions about the security of the site there is usually an email or phone number to contact.
- Consider keeping a bank account just for online purchases rather than using your primary bank account for online transactions.
- Ensure that the site is protected by VeriSign or another security company.
- When shopping, only do business with websites supported by SSL technology. A small lock or key will show in the bottom of your browser window if it is SSL encrypted.

Online Discussions

- Do not use your Webster email as these groups rarely guarantee the protection of your email.
- Do not provide any personal information on message boards or in discussions.
- Do not download questionable applications linked in discussions, they can potentially contain harmful material.

General Tips

- Never give out financial information such as your bank account number or credit card number over the phone or via email.
- Do not share your passwords over the phone or via email with anyone claiming to be a company representative.
- Use “good” passwords, not ones easily guessed or hacked (use numbers, letters and other characters in your password and keep it secret).

REMEMBER: Using good internet security practices protects not only your computer but your identity as well.

A Note To Resident Students:

If you suspect that your machine has become infected by a virus or other potentially harmful material, you can contact ResTech for service of your machine.

Call x5995 or visit

www.webster.edu/helpdesk/restech to setup an appointment.