Safe Computing

WITHOUT MY COMPUTER I CAN'T DO MY SCHOOL WORK!

HOW CAN I KEEP IT SAFE?

What's the worst that could happen?

Neglecting your computer, leaving it open to viruses, spyware and other malicious software can have dire consequences. An ailing computer can stop you from finishing assignments, corrupt your seminar papers, and prevent you from emailing faculty and fellow students. If you live on the residence campus and your computer begins affecting the Simmons network, your Internet access will be limited, preventing you from completing homework or sending email from your room. And, a virus on your USB memory device can destroy files on it and on your computer.

What do I need to do?

Visit my.simmons.edu/disinfect-protect and follow instructions to:
- Install free antivirus software with current virus definitions
- Run critical updates on your operating system
- Remove malicious software like spam and spyware
- Secure your computer with a username and password
- Remove file sharing software

Save time: do it now

It takes between 30 minutes and 2 hours to disinfect and protect a computer in relatively good condition. It will take many more hours of your time, or a good chunk of money to pay someone else, to fix a computer riddled with viruses. Restoring your papers and presentations may turn out to be impossible. Don't wait until everything is due and you cannot live without your computer. Save yourself some unnecessary stress; go to my.simmons.edu/disinfect-protect now.

Technology at Simmons College

Protect yourself. Protect your information.

Protect your personal information

Beware of giving your personal information on the Internet (e.g. via email, IM, or a web site). Follow these steps to ensure your safety:
- If asked to supply your mother's maiden name, do not provide the real one. Make note of any false information you have supplied for future reference.
- Do not supply your social security number.
- Think about who is looking at your profile or page on Facebook or MySpace: faculty, family, future employers, strangers?

Beware of Phishing

Phishing is a method to trick you into revealing personal information. The scheme starts by sending you an email purporting to be from a business like a bank, or ISP. If you respond by replying or filling out the form, you put your money and identity at risk. Be suspicious. Examine messages and URLs carefully. Call the business using a number you know to be legitimate, or delete the message.

Avoid file Sharing / peer-to-peer

When you use file sharing services, you risk violating copyright laws, the health of your computer, and the privacy of all information you have stored on it. Common file sharing applications are: LimeWire, Bearshare, BitTorrent, Edonkey, iMesh, Kazaa, and Morpheus. Simmons urges you not to install any of this software on your computer. For more information, visit my.simmons.edu/filesharing

Never share your passwords

Your passwords are the keys to your identity: don't share them with anybody. No one has a legitimate reason to ask you to tell her/him your password, including Simmons Technology staff. Do not write passwords down. Create passwords you can remember, and that are difficult for other people or systems to guess. When you're finished, always log out of email, IM, Simmons computers, etc.

Need help?

First try my.simmons.edu/disinfect-protect, or my.simmons.edu/technology/students. The Simmons College Technology Help Desk is available by calling 617-521-2222, option 8, or by sending email to helpdesk@simmons.edu

Need a new computer or software?

Visit my.simmons.edu/technology/purchasing for access to our online Dell, Apple, and e-academy stores for substantial savings. You will need your Simmons username and password. Buy Office and other Microsoft products at 50-90% discounts through our new arrangement with e-academy.

my.simmons.edu/technology/students - click "safe computing"