Security Tips

# NEWSLETTER

MCC ETS EDUCATIONAL TECHNOLOGY SERVICES

Communications and Network Services

## Seven Practices for Safer Computing

**1. Protect your valuable personal information**

Your Personal Identifiable Information (PII) can provide identity thieves instant access to your financial accounts, credit record, and other assets. Since anyone can be a victim of identity theft, here's how to stay safe:

1. Avoid phishing scams
2. Don't give out your PII unless you know how it's going to be used and that it's protected
3. When shopping online, don't enter any PII unless you know the website is secure
4. Read and understand website privacy policies

**2. Know who you're dealing with**

Unfortunately, you must be aware of dishonest people on the internet. Before doing business through an unfamiliar site, do your research. File-sharing allows access to a breadth of information, music, games, and software. It is also opens up your computer to a large amount of harmful viruses and malware.
For important information, visit **http://www.rochester.edu/it/security/yourself/file-sharing.html** .

**3. Use security software that updates automatically**

To prevent your computer from being taken over by malware and/or spyware, you should have, at minimum, anti-virus and anti-spyware software, and a firewall. Make sure that your security software is up to date by setting the preferences so your software updates automatically.

**4. Learn about the security features of your operating system and Web browser**

Hackers take advantage of web browsers, such as Internet Explorer, and operating system software, such as Windows, that don't have the latest security updates. It is critical to set your operating system and Web browser software to automatically download and install company-issued security patches.

Another way to protect yourself from hackers is to disconnect your computer from the internet when you're not using it.

**5. Protect your passwords**

Keep your passwords in a secure place and don't share them with anyone.

Visit **http://www.rochester.edu/it/security/yourself/passwords.html** for more information on password protection.

**6. Back up important information**

No system is completely secure. Any important information should be backed up on some sort of removable memory, such as a CD, external hard drive, or flash drive, and stored in a safe place.

**7. Know what to do in an e-emergency**

If you suspect malware is lurking on your computer, stop shopping, banking, and other online activities that involve user names, passwords, or other sensitive information. The malware could be sending your information to identity thieves. Contact the appropriate authorities, such as the FBI or the Federal Trade Commission, concerning any suspicions of identity theft or fraud.

**UnivIT_SP@ur.rochester.edu**.