Internet and Email Security

Phishing Scams

While phishing scams are not new, they are becoming more and more sophisticated. These high-tech scams use spam or pop-up messages to trick users into disclosing credit card numbers, bank account information, Social Security numbers, or other confidential information. To learn more about phishing as well as other Internet threats visit *makeitsafe.missouri.edu/phishing.html* and *makeitsafe missouri.edu/spyware.html*.

Abusive Email

Abusive email can take many forms, ranging from the merely annoying to personally offensive to outright threatening. They may arrive in the form of advertising, junk mail, or spam, but all are inappropriate. What should you do if you receive problem or abusive email?

- Be cool. Don't reply to the email, do not delete or archive immediately.
- Be skeptical. If it sounds too good to be true, it probably is!
- Be quick about reporting. Report any problem email as soon as possible.

To report suspected problem or abusive email, contact *abuse@missouri.edu*.

Property Registration

For Bicycles and Electronics

1. Go to mubsweb.missouri.edu/mupd/
2. Log in with your MU PawPrint and password. If you cannot log in, please wait one week and try again or email the Crime Prevention Unit at *mupd@mupolice.missouri.edu*
3. Follow the onscreen instructions.
4. Complete the MU Police registration process:
   - Electronics: MU Police Registration is complete when the electronic form has been submitted.
   - Bicycles: Print the registration form. Bring it to the MU Police Department (Virginia Ave. Garage) to be issued a sticker. Affix the sticker to your bike.

Police Department
University of Missouri - Columbia
mupd@mupolice.missouri.edu
(573)882-7201

IT Security for Students

Information technology security is vital to the University of Missouri.

By working together, everyone in the University community benefits from a computing environment that's reliable, safe, and trustworthy. Remember, you can help us

Make it Safe

makeitsafe.missouri.edu

Information Security and Access Management
Division of Information Technology University of Missouri
615 Locust St., Columbia, MO 65211
ISAM@missouri.edu • (573)882-2000

Social Networking

Do you use Facebook, Twitter, MySpace, or other Social Networks? Social networks are a great way to share common interests or stay in touch with friends and family online, but you need to be careful when using them.

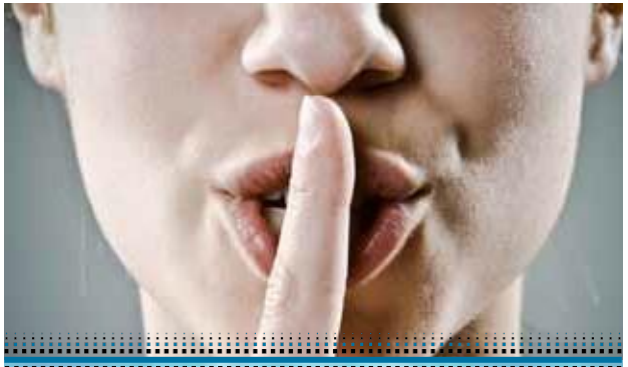
Top five threats on social networks:

- Cyber bullying, stalking, and sexual predators
- Vulnerabilities in applications and widgets
- Phishing and spam
- Collection of personal data
- The fake profile or "evil twin"

Top five security measures:

- Set privacy defaults.
- Be careful with third party applications and widgets.
- Limit personal data posted, such as your birthday or address.
- Only accept friend requests and connections from people you know directly.
- Consider all information and pictures you post as public!

makeitsafe.missouri.edu/community-networking.html



Password Safety and Security

One of the most basic and important principles of information security is password safety. Your password is the major form of protection for your computer account, your data and the University resources that you access.

An easy way to form a secure password that you can remember is to think of a phrase, song, poem, or sentence and use the first letter from each word. For example:

" I moved to Chicago in '98!"="ImtCi98!"

Once you have created a secure password, you need to keep it safe. Here are some things you can to do to help protect your password:

1. Never share your password with anyone.
2. Change your password at reasonable intervals.
3. Do not write down your password.
4. Don't use your Login ID and Password for non-University Web sites and services, such as online banking.

makeitsafe.missouri.edu/passwords.html

Physical and Workstation Security

Physical Security

There are a variety of easy things you can do to physically protect your computer and your data.

- Don't leave your laptop unattended.
- Lock your door when you leave your room.
- Make periodic backups of your data.

Workstation Security

Here are some steps that can be applied to help secure any system, especially your home computer that is connected to the University's network.

- Set a secure administrator password.
- Enable the operating system firewall.
- Keep your machine current by installing operating system updates.
- Install an anti-virus program and keep it up-to-date.
- Be cautious about what you install.

makeitsafe.missouri.edu/best-practices/