3 Easy steps to protect yourself online.

THE UNIVERSITY OF IOWA

1 Look before you click.

Links Sent By Friends -- Don't assume that a link to a website/file is harmeless because it was sent to you by a friend. The link could point to malicious content. Compromised computers can infect other machines with that malicious software.

Away Messages -- Don't click on any links in away messages. Some malicious programs will add a link to an Instant Message's (IM) away message. Anyone who clicks on this link could compromise their computer's security.

Suggestion: Verify with the person who sent you a link that they really meant to send it. Also, if you've clicked on a link that is supposedly to pictures, a web browser should open and display the pictures. If you click on a link that should open a picture, and a box opens asking you if you want to "open", "run" or "save" something, cancel it immediately!

2 Don't accept file transfers you aren't expecting.

Possible Consequences -- If you do, you could be downloading malware that could make your computer unstable, be used to steal your personal information, and/or be used to attack other computers.

Files Sent By Friends -- Don't assume that a program/file is safe because a friend initiated the transfer. Many cases of infected computers are due the result of malware spread through the IM software on that computer. Therefore, if your friend's computer is compromised, a malicious program may send you an IM that appears to have been deliberately sent by your friend.

Suggestion: If you receive an offer to accept a file transfer, contact the sender to verify that they just sent you an offer to download a file.

3 Don't give out personal/sensitive information over Instant Messaging clients.

Chats Are Usually Not Encrypted -- Instant Message conversations are almost exclusively unencrypted. This means that when the conversation is being transferred over the network, it is in clear text. If someone captured or viewed the conversation while it was in transit, they could easily read it. For example, if you were to give out your Social Security number and a few personal details while Instant Messaging, a malicious user could intercept this information. They may then use it to assume your identity and commit various forms of fraud.

Shoulder Surfing -- Perhaps you're talking to a friend via IM and you divulge some personal information. Your friend may be in a public, or a semi-public, place without your knowledge. If your friend is not careful, someone could walk by and read your conversation/personal information.

Logging -- Sometimes people turn on logging for the conversations that they have. If you discuss/share any personal information, it will be stored on the person's computer in a log file. This creates a chance that someone, possibly malicious, could access these log files and obtain your personal information.

Suggestion: Do not liberally give out your personal information. If for some exceptional reason you must give out personal information, insist that it be done in a secure manner. Consider alternate ways of sharing private information, e.g. calling the person.

Further Recommendations:

- o If your IM client supports it, configure your options to only allow/accept messages from people you know.
- o Certain clients, notably IRC (Internet Relay Chat) clients, automatically accept file transfers. If your client provides an option for this functionality, turn it off.

For more information visit: http://itsecurity.uiowa.edu or contact the ITS Help Desk at 384-HELP (4357) or email: its-helpdesk@uiowa.edu