Password Guidelines

1. Your first line of defense is your password. Without a good, strong password, your machine and the data stored in it are vulnerable to hackers. Here are some basic guidelines you should keep in mind:

- Change your password at least every 3 months
- Never use your name, address, or login id as your password
- Never share your password with anyone, including your relatives, administrative assistant, or technical support personnel
- Passwords should be easy to type and easy to remember (so you don’t have to write it down)
- Use at least 3 of the following classes of characters: uppercase letters, lowercase letters, numbers, punctuations marks and special characters. For example: c@ts+dog5.

Anti-Virus Protection

2. Computer viruses are becoming more and more aggressive. They spread exponentially to the point of making the Internet not usable. Infections threaten not only your personal computer, but the entire University network infrastructure. Some varieties find and distribute files containing sensitive information stored in your machine. Others simply destroy all the data you have stored.

Symantec Endpoint Protection software is provided free of charge to all faculty, staff, and students. Visit USF’s Security Website, http://security.usf.edu, for instructions on how to download and install your copy of SEP.

Email

Email is a fundamental part of today’s work at USF, but it is also a source of many problems.

Email Viruses: One of the preferred means of propagation for viruses is through email. An infected computer will send a copy of its virus to all users on that computer’s address book. As a rule, NEVER open attachments from a stranger. Not only that, be highly suspicious of attachments sent by friends or family. Only open attachments you are expecting to receive.

Phishing: Phishing is a method by which hackers send you fake emails, posing usually as a bank, trying to get you to volunteer your personal information. They may, for instance, say they represent Citibank and you need to go to their web site to update your records. Some phishing emails look very official. Check out FraudWatch International at http://www.fraudwatchinternational.com

Spam: Spam is the word used to describe unwanted mail. The term is most often used in association with unsolicited commercial emails, UCE. Never retaliate against the sender of UCE using ‘Reply’ or ‘Reply-All.’ Often this will simply make things worse. Avoid having your email address published on any web pages.

Spammers use automated software called bots to harvest email from web pages. Instead, use something like “jdoe at usf.edu.” Finally, check out the web site for major spam reporting services, such as http://spamcop.net or http://spam.abuse.net.

System Updates

It is important to keep your system updated regularly. We suggest that desktop owners set their machines to perform automatic daily updates.

If you have Windows XP, click on the Start button and right-click on My Computer. Click on Properties and then the Automatic Updates tab to set a daily schedule.

For Mac OS, click on System Preferences from the Apple menu. Click on Software Update from the View menu and click the radio button for Automatically. Click on the daily interval option.

Reporting an Incident:

University of South Florida Incident Response Team
4202 E. Fowler Ave, LIB618
Tampa, FL 33620
Phone: 813-974-2287
E-mail: abuse@usf.edu