GUIDELINES FOR USE OF USC COMPUTERS

UNIVERSITY TECHNOLOGY SERVICES

PROTECTION STARTS WITH YOU.

Here are 4 simple things you can do to protect your USC computer and data.

1. AVOID PERSONAL WEB BROWSING.

This puts any data you handle at higher risk. Even a normally trustworthy website can unknowingly spread a computer virus.

Fact: USC computers have been infected by visiting news websites, Facebook, community organization websites, and many other websites unrelated to USC business.

2. DO NOT GIVE YOUR USC PASSWORD TO ANYONE!

Don't even share it with coworkers, your supervisor, or a computer technician. Only use your USC password to log in to familiar USC systems.

Fact: In 2011 more than 100 USC faculty and staff members were tricked by criminals into divulging their passwords, by various means, including fake email notices and fake login web pages.

3. AVOID PERSONAL SOFTWARE AND DATA.

As with personal web browsing, usage of personal software on a computer raises the level of risk to the business data on that computer. Obtain the approval of your supervisor or IT support staff before placing personal software or data on your business computer. Every software package has security bugs. Each additional security bug on a computer places all data on the computer at a higher level of risk.

Fact: File sharing software is often targeted by criminals as a means to infect computers, or to steal files that are accidentally shared.

4. DO YOU WORK WITH SENSITIVE DATA?

If you work with Social Security Numbers, grades, financial information, medical information, or research data, please note:
If your computer becomes infected, you must contact UTS Security immediately (email *security@sc.edu* or phone 803-777-1800). Do not attempt to remove the infection, and do not move files or software from the computer. If a Security investigation is required, any changes to the computer will interfere. Here are some other special considerations:

- Do not send sensitive data through email.
- Only retain sensitive data for as long as is truly required to perform your job functions.

Fact: In many security incidents, USC Employees have removed or copied some of the software or data from an infected computer. In 2011 UTS Security performed 25 computer investigations. In every case where a user made changes to the computer, the time required for investigation was increased, and findings of the investigation were more severe.

FOR IMPORTANT DETAILS, SEE THE INFORMATION SECURITY PROGRAM WEBSITE AT: SECURITY.SC.EDU.

Myth versus Fact

Myth: Security technologies provide the best means for protecting a computer and data.

Fact: An overwhelming majority of Security incidents at USC have root causes related to computer usage and management.

Myth: If my computer becomes infected I will notice the change quickly.

Fact: It is common for a computer virus infection to go unnoticed for months or years.

UNIVERSITY OF SOUTH CAROLINA
University Technology Services