



University of South Alabama

# **Computer Services Center: An Introduction**

---

**By: Andy Lightbourne  
Associate Director for Academic Computing  
Computer Services Center  
251-460-6161**

# Welcome!

The Computer Services Center (CSC) supports a wide range of computing and network services throughout the University. These include the core University student information and financial systems under Banner; hospital and clinical data processing; the University networks (wireless and wired); Internet access and email; University telephone systems; and many others. Operating groups within our organization are located at the main Computer Services Center building, Telecommunications, and various Hospital sites.

The primary CSC point of contact for faculty is the Academic Computing group, which focuses on support of instructional and research computing, as well as providing general computer problem assistance. The Academic Computing office and general help desk support is open on normal business days (Monday through Friday) from 8-5 and may be contacted at 460-6161 or via email at [acad@jaguar1.usouthal.edu](mailto:acad@jaguar1.usouthal.edu).

The CSC operates 24x7, 365 days a year. Although CSC staff have voice mail on their individual lines, the 460-6161 number is always answered by a human. During regular business hours, the receptionist staff will route your call appropriately. Outside of these hours, the phone is answered by the machine room computer operators. On-call staff can be paged for critical issues; matters which can be deferred to business hours can be logged into our trouble ticket system.

Among the services that Academic Computing provides the faculty, staff and students at the University of South Alabama are:

- Jaguar1 (primarily student) and GroupWise (primarily employee) Email
- Symantec Antivirus Software
- DormNet - Student Dormitory Network
- Coordination of SAS and SPSS Statistical Package licenses
- Computer Workshops
- Computerized Test Scoring (in conjunction with CSC Scheduling Services)

More information is available at our web page, <http://www.southalabama.edu/csc>

During the year the CSC offers free workshops for faculty and staff. Typical topics include:

- Basic Computer Skills: An Introduction to Microsoft Windows XP
- Protection of Data and Antivirus Software,
- E-Mail: GroupWise
- Windows Security
- Multiple courses on Microsoft Office products, including Word, Excel, and PowerPoint
- Introduction to DreamWeaver

**University of South Alabama**

Home | Index | Search | Directories | FAQ

## CSC Computer Workshops

Academic Computing will conduct the following computer workshops throughout the Spring 2005 Semester. Although our courses are offered free of charge as a service to USA faculty and staff, advanced registration is required. You may register by calling the Computer Services Center at 460-6161 or via email. To register by email, please send a message containing your name, department, and telephone number, and your choice of classes and dates to [seminars@usouthal.edu](mailto:seminars@usouthal.edu).

### Introduction to Microsoft Windows XP

This course will introduce users to the basic features of Windows 9x and XP. You will learn to perform basic tasks such as how to start and stop programs, manipulate windows, customize the desktop, manage files in Windows Explorer and identify the functions of the Active Desktop. Instructors: Aaron Long and Susan Allison Lee

**January 24, 2005, Monday, 1:00 p.m. - 4:30 p.m.**  
**January 28, 2005, Friday, 8:30 a.m. - 12:00 p.m.**

Prerequisites: None

### Protection of Data and AntiVirus Software

This course will outline essential procedures for protecting your data. Learn to backup your files and set up a convenient backup schedule for

**Quick Select:**

- Select a Workshop
- Select a Workshop
- Introduction to Microsoft Windows XP
- Protection of Data and AntiVirus Software
- E-mail: GroupWise 6
- Spyware, Phishing and Trojans ... oh my!
- Windows Security
- Introduction to Microsoft Word XP
- Introduction to Microsoft Powerpoint XP
- Introduction to Microsoft Excel XP
- Introduction to DreamWeaver 6

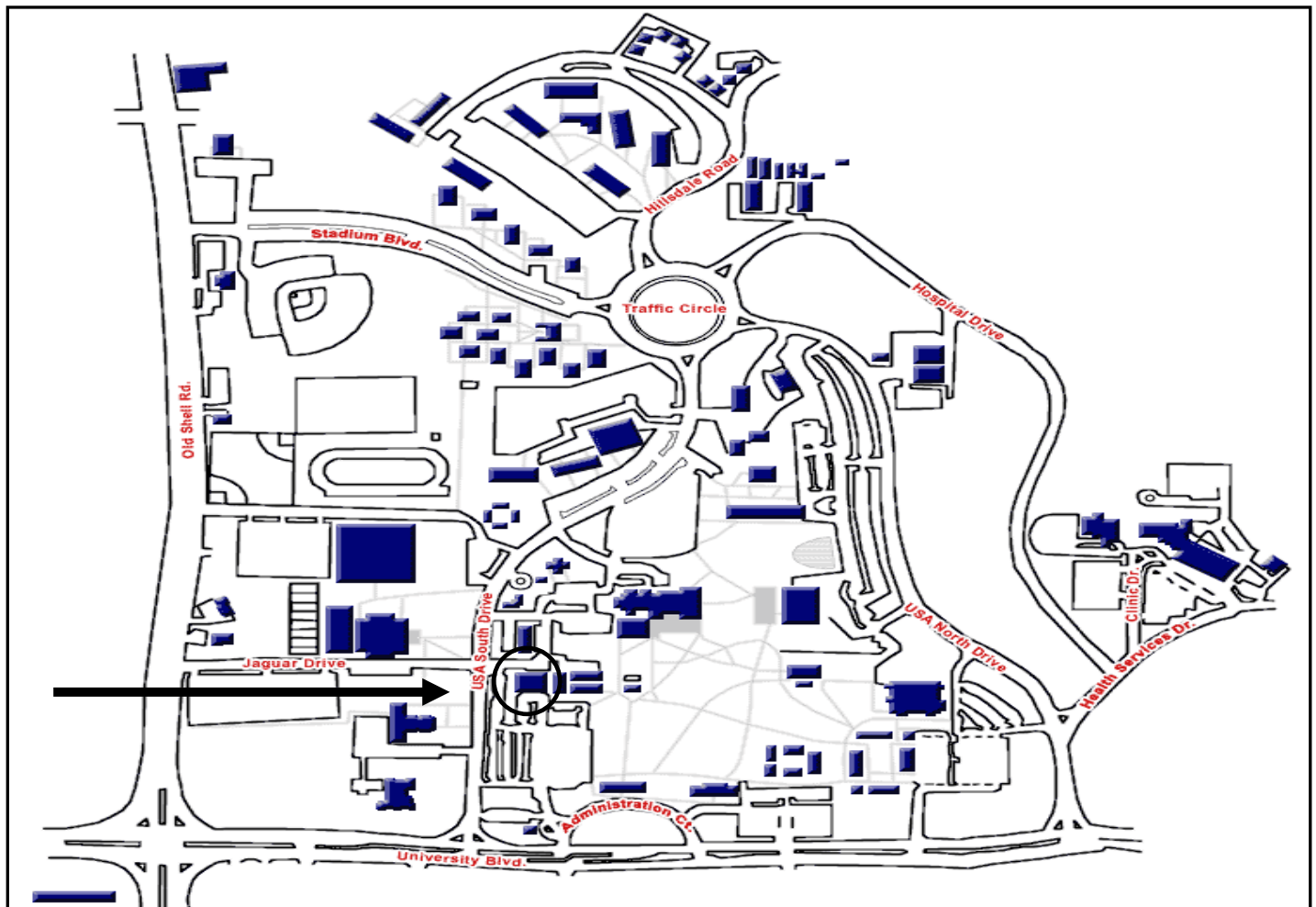
This web page now includes a link for self-registration by employees. We also send out a campus-wide email at the beginning of each term. Further information on workshops can be obtained by emailing [seminars@usouthal.edu](mailto:seminars@usouthal.edu).

## Finding the CSC building



**Computer Services Center**

If you need directions please call us at 460.6161. You may access the campus map at <http://www.usouthal.edu/maps/maincampus.html> .



## GroupWise

GroupWise is the primary email system used by University faculty and staff. GroupWise can be accessed by the GroupWise “native client” program loaded onto your computer, or through Web Mail. GroupWise also supports a wide range of PDAs and “smart phone”, including BlackBerry. GroupWise also provides a number of group productivity features, such as shared calendars and “proxy access”.

**GroupWise Email Information: <http://groupwise.usouthal.edu>**

**GroupWise Email Home Page**

Welcome to the official USA GroupWise Email Information Page. Email accounts are available to all faculty and staff at the University of South Alabama. GroupWise is the most common email system among university employees, however you have the choice of either a Jaguar1 or GroupWise email account.

**Read the FAQ!**

Most common questions regarding GroupWise are answered in the [GroupWise FAQ](#). Please check there before calling the Computer Center; it may save you time.

Having trouble with Viruses or Spyware? Go here for help: [ACAD Help Page](#)

**Requesting a GroupWise Account**

[Click here for information on how to request a GroupWise email account.](#)

In addition to individual email accounts, accounts may be requested for use by a group, organization, or department. These may be on the GroupWise or jaguar1 system. For example, [president@usouthal.edu](mailto:president@usouthal.edu) , [registrar@usouthal.edu](mailto:registrar@usouthal.edu) , [history@jaguar1.usouthal.edu](mailto:history@jaguar1.usouthal.edu).

Some departments use the jaguar1 email system, which does not have a “native client”, but supports a range of IMAP clients including Microsoft Outlook, Thunderbird, Apple Mail, etc. Jaguar1 has web mail, but does not support PDAs. The jaguar1 information portal is at <http://jagmail.usouthal.edu> .

## Jaguar1 FAQ: [http://jagmail.usouthal.edu/jagmail/jagmail\\_faq.htm](http://jagmail.usouthal.edu/jagmail/jagmail_faq.htm)

The screenshot shows the University of South Alabama website with a red navigation menu on the left. The main content area is titled "Jaguar1 FAQ" and is divided into two sections: "Setup" and "Management".

**Setup**

- [HELP! I can't figure out how to setup/access my email account.](#)
- [How do I setup Netscape or Mozilla to access my Jaguar1 email?](#)
- [How do I setup Outlook Express to access my Jaguar1 email?](#)
- [What is the difference between my Jag Number, PIN, User ID, and Password?](#)
- [My userid/password does not work.](#)
- [I keep getting a timeout error when I am trying to access my email using the Web Mail interface.](#)
- [Can I use the Web Mail interface via an secure/encrypted connection?](#)
- [How do I know if my Web Mail session is secure/encrypted?](#)

**Management**

- [How do I read my email?](#)
- [How do I request a Jaguar1 account?](#)
- [I forgot my password, how do I access my email?](#)
- [How do I change my password?](#)
- [How do I cancel my email account?](#)
- [I can read my mail messages but when I click the Compose, Reply, Forward or Help buttons nothing happens. What's the problem?](#)
- [How do I forward my Jaguar1 email to another email account?](#)

## Symantec Antivirus Software: <http://www.usouthal.edu/csc/sav>

All computers should have some sort of antivirus software that is regularly updated with the latest virus definition files. The University of South Alabama Computer Services Center is participating in an Educational Site License Program with Symantec Corporation, the makers of Symantec Antivirus Software (a.k.a. SAV). As a result, SAV may be installed on all University-owned computers without charge to the department or user. Click on the **USA Symantec Antivirus Program** link and follow the download instructions.

SAV is available for Windows XP and Windows Vista. A major feature is the ability to **automatically update definition files** from the University's SAV servers. (If you take your laptop off-campus, it can be updated from Symantec over the Internet).

The screenshot shows a Microsoft Internet Explorer browser window displaying the "Symantec Antivirus Software" page. The page has a red navigation menu on the left and a main content area with a blue background.

**Symantec Antivirus Software**

All computers should have some sort of antivirus software that is regularly updated with the latest virus definition files. The University of South Alabama Computer Services Center is participating in an Educational Site License Program with Symantec Corporation, the makers of Symantec Antivirus Software (a.k.a. SAV). As a result, SAV may be installed on all University-owned computers without charge to the department or user.

NOTE: This contract does NOT extend to personal home computers. The automatic update feature of this software will not work on computers outside of the USA network.

SAV is available for Windows 98, Windows Me, Windows NT, Windows 2000 and Windows XP. New features include the ability to **automatically update definition files**. Once SAV is installed you do not need to run any sort of weekly download or update. Windows 95 users cannot install SAV. They should upgrade to Windows 98 or higher before installing SAV.

- [Installation instructions for Windows 98/ME](#)
- [Installation instructions for Windows NT/2000/XP](#)

**Read the FAQ!**

Most common questions regarding SAV are answered in the [SAV FAQ](#). Please check there before calling the Computer Center, it may save you time.

• Click on the **Installation instructions** for your computer's operating system link

Follow the installation instructions to install the correct software version for your machine.

# Ten Things You Should Know When Using Your Computer

## I. Remember your Antivirus software and keep it updated.

It's not enough to have the software installed (If you don't have an Antivirus package, stop reading right now and get one!); you also need to keep up with new viruses as they emerge. "Your Antivirus software is only as good as your latest virus definitions set," says Kelly Martin, senior product manager for Symantec's Norton Antivirus. (using the CSC-provided SAV license automatically does this for you, but it never hurts to check the signatures dates periodically. They should never be more than a week old.)

## II. Keep your operating system patched.

E-mail-born worms and other scourges like to exploit security holes in your software, namely Windows and other Microsoft programs. These days Microsoft issues critical updates to fix these flaws. Several years ago, the Slammer worm exploited a vulnerability that Microsoft had fixed more than six months before. But thousands of infected computers--including some at Microsoft--didn't have the patch installed. Run the Windows Update program **once a week** and whenever Microsoft issues a warning. Better yet, set up automatic Windows updating.

## III. Don't trust files even from your friends.

You get a message you think is from a friend with what looks like a cool file attached, so you click on it. Next thing you know, you're Typhoid Mary, spewing out infected e-mails to everyone in your address book. That's how the Sobig.F worm spread--and it happened so quickly that millions of copies got out before the Antivirus companies could update their databases.

"Never trust an e-mail 'from' address," adds Chris Wysopal, director of research for security consultants @Stake. "And **NEVER open an attachment without verifying it was sent by a trusted person and they meant to send it to you.**"

## IV. Spyware and pop-ups.

Like Trojan horse programs, spyware secretly installs itself when you download software like file-swapping applications; it tracks your movements online and delivers ads based on where you surf. Pop-up ads can also exploit security flaws in Internet Explorer, like the recent Qhost Trojan that hijacked users' browsers after they viewed an ad on the Fortune City Web site. More Information on spyware and some steps for removing it, can be found at <http://patches.usouthal.edu> .

## V. Just delete all spam.

Unsolicited commercial e-mail is more than just a nuisance; it's also a major source of virus infections. In fact, some versions of Sobig are designed to turn infected PCs into zombie machines that can be used to send spam.

## VI. Avoid bogus file downloads.

Be wary of any Web site that requires you to download software to view a page, unless it's something familiar like a Flash plug-in or Acrobat Reader. The file may contain a virus, a Trojan horse, or some auto-dialer that calls pay-per-minute numbers via your modem and racks up huge charges. "**Do not install software via the Web unless you are absolutely sure what it is and that you trust the company you are downloading it from,**" warns @Stake's Wysopal.

## **VII. Make a rescue disk and keep it handy.**

When things go bad, a boot or rescue disk is your first step to recovery. At minimum, you'll want to put the basic elements of your operating system on a floppy disk or Zip media, so you can bypass the hard disk at startup. Use your Antivirus program to create a rescue disk you can use when your system gets infected. Label it with a date and store it near your system where you won't lose it.

## **VIII. Don't take the phishing bait.**

Phishing is the practice of sending out fake emails, or spam, written to appear as if they have been sent by banks or other reputable organizations. The intent is to lure the recipient into revealing sensitive information such as user names, passwords, account IDs, ATM PINs or credit card details. Typically, phishing attacks will direct the recipient to a web page designed to mimic a target organization's own visual identity and to harvest the user's personal information often leaving the victim unaware of the attack. Obtaining this type of personal data is attractive to black hats because it allows an attacker to impersonate their victims and make fraudulent financial transactions. Victims often suffer significant financial losses or have their entire identity stolen, usually for criminal purposes.

Starting in 2008 phishers began aggressively targeting higher education populations, asking for email accounts and passwords, and then using those passwords to log onto University web mail systems and push spam messages through them. These attacks often embody realistic University information.

***NEVER provide a PIN, password, or Social Security Number through email – even if requested. A request for this information through email is ALWAYS bogus. The Computer Services Center NEVER asks for this information through email.***

## **IX. Use a firewall.**

A firewall is like a bouncer for your computer--it checks every ID at the door and won't let anything in or out until you give the thumbs up. So a hacker can't access personal information on your hard drive, and a Trojan horse keystroke logger (a stealth program that monitors the characters you type) can't steal your passwords and transmit them over the Net. Windows XP and Vista have good built-in firewalls, and will alert you if the firewall has been disabled.

## **X. Make backups and keep them safe.**

Simply put: Back up your data files at least weekly (daily if you're running a business). Even if you fall victim to a virus or hacker attack, you'll escape with only minor damage.

**Do Not Keep Backups on Floppy Disks!** They were designed for transporting files from one place to another but never long time storage. Backups should be done on CD's, Servers, flash drives or other stable storage.