



Introduction

Your work computer is the property of San Jose State University and is provided for you to be able to perform your job. As such, your computer is not really “your” computer, and you should minimize personalizing it with screensavers, games and software not provided at the time of installation.

There are many ways your computer can become compromised in our current computing environment. The negative effects of being compromised can range from annoyances like pop-up windows covering your screen every time you turn on the computer, or browse the Internet to keyloggers that capture your keystrokes and screen data, and mirror them back to a remote site.

Do's:

- If you see an icon that shows Microsoft Windows updates have been downloaded and are ready to install, please click the icon and allow the updates to install.
- When you walk away from your computer, lock the console by pressing Ctrl-Alt-Delete simultaneously, and then choose Lock Workstation. This will prevent other people from using your open sessions in PIMS, email, or PeopleSoft. It will also prevent other people from being able to install software or access information to which they are not entitled.
- Report any problems to Administrative Technology staff as early as possible. The people to contact depend upon your department:
- Feel free to call any Administrative Technology staff members if you are unsure about a pop-up message or an email that you received. You can call any of the people below, or send an email to admtech-group@sjsu.edu. This will automatically be distributed to the entire Administrative Technology desktop support staff.

Primary Contacts (feel free to call anyone if the primary is not available):

- Bursar's Office, HR – Chris Bradford (4-1545) Christopher.Bradford@sjsu.edu
- Computer Center, FD&O – Kane Imai (4-1664) Kane.Imai@sjsu.edu
- UPD – Nancy Ashley (4-1716) Nancy.Ashley@sjsu.edu
- Everyone else in the Division of Administration & Finance – Jerry Crawford (4-1953) Gerald.Crawford@sjsu.edu
- Athletics – Paul Leung (4-1573) Paul.Leung@sjsu.edu

Don'ts:

- Don't visit websites that are not related to your job functions at San Jose State University, or that you are not certain are bona fide websites. There are a few sites on the Internet that can take over your computer and/or plant spyware just by visiting their homepages. Generally commercial sites like Yahoo, MSN, AOL, and Google are safe. When in doubt, don't visit the site.

- If you mistype a website page name and get redirected to a site that generates a pop-up asking if you want this page to be your new home page, choose NO, and navigate away from that page or close the page without responding if that is an option.
- Don't install your own software (this includes games, holiday screen savers, instant messaging clients, or anything else not licensed by the University). If you need an instant messenger to communicate with your coworkers, ask an Administrative Technology staff member to install it.
- Don't double-click on any email attachments to launch them directly from email. If you are expecting a legitimate attachment, download it to a directory on your pc and scan it for viruses prior to opening it. NEVER double click an attachment ending in .pif, .exe, .com, .scr, or .ctl. These are all executable files and in 90% of the cases they are worms or other types of unwanted system compromises.
- Don't click any links from unsolicited mortgage offers, bank verifications, or attachments purporting to detect and rid your computer of unwanted spyware.
- Don't open any attachments purporting to be updates from Microsoft. Microsoft does not email updates or fixes, and they do not have your email address.
- Don't automatically install a "helper" application when prompted by a website if you are trying to open an attachment and your computer doesn't have software that opens it for you.
- Don't provide your username and password in response to any email requests irregardless of how legitimate the email may appear to be. These are phishing scams that attempt to collect your login credentials that can then be used to cause harm or compromise your identity.
- Don't take advantage of web offers to block pop-ups, spyware, etc on your SJSU-owned PC. Many of these offers route all of your transactions through a proxy server that captures all of your online activity. In the near future, CMS will be blocking access attempts from these proxies.