



- Set good passwords.

If you think someone's guessed your password, change it immediately.

- Keep your software up-to-date.

New versions are released to counter the latest threats.

- Run anti-virus software.

You should set it to check for anti-virus software updates at least once a week.

- Be careful opening e-mail attachments.

Viruses are often transmitted as attachments to e-mail messages.

- Control access to your computer.

If you don't know who's accessed your computer, it's not secure.

- Routinely back up your files.

By backing up files you can recover them if they are corrupted or destroyed.

- Turn off your computer when you leave for the day.

Your computer can't be invaded if it's not connected to the network.

- Install screen-saver passwords.

With screen-saver passwords, no one can look at your monitor unless they know the password.

- Clean your hard drive before disposing of it.

Deleting files is not enough; over-writing confidential material with random input is best.

- Take extra care with your laptop or other portable devices.

Don't plug a portable device into the network if it isn't updated with the latest patches and scanned for viruses.

WHO CAN HELP

For more information and assistance with IT security related issues:
Visit the UCOP IT Security Web site at
<http://www.ucop.edu/irc/itsec/>

Talk to your departmental PC Coordinator.
Contact IR&C Policy Director Jacqueline Craig at
Jacqueline.Craig@ucop.edu or (510) 987-0409.



Information Resources and Communications
University of California Office of the President
<http://www.ucop.edu/irc>

February 2005

Do You Work for UC? Then Security Is Your Business



GUIDELINES FOR HELPING SECURE
THE UCOP COMPUTING ENVIRONMENT

Computer Security

YOU HAVE A ROLE

In this age of electronic intrusion and theft, it is essential for the University to protect its administrative data and intellectual property. Further, the University has a profound commitment to protecting the confidential and personal data it holds pertaining to employees, students, alumni, patients, donors, etc. Personal information includes Social Security numbers, financial account numbers, and patient health data, as well as someone's name in combination with payroll information, home address, or home phone number.

Everyone—from associate vice president to secretary, from administrative analyst to division head—has an important role to play in security. Remember, when you take steps to secure computers and data, you are protecting the heart of the University itself—the information associated with teaching, research, patient care, and public service.



DON'T BE SHY: REPORT!

Suspicious Incidents

If you think you've experienced a security incident, report it immediately to your supervisor.

Strange Computer Activity

If you observe strange activity on your computer, report it to your departmental PC coordinator. For example:

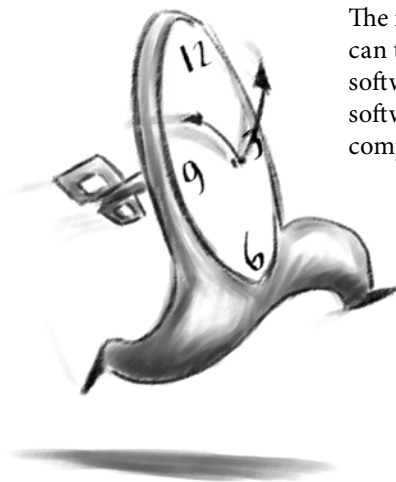
- You notice strange files left on your desktop or in your folders
- Unexpected windows pop up on your screen
- Your Web browser opens to a page other than the default you selected

Security Breaches

If a breach occurs to the security of any computer, laptop, or other portable device holding *confidential or personal data*—such as names in combination with Social Security numbers—report the breach to the Associate Vice President—IR&C within 24 hours after discovery.

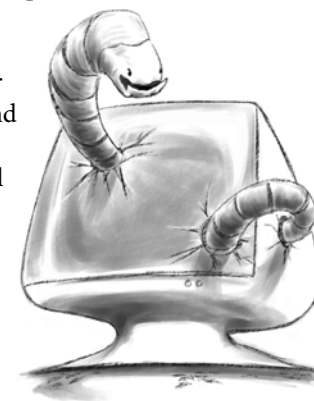
KEEP UP-TO-DATE

The most vital action you can take is to update your software routinely. If your software isn't current, your computer is vulnerable to attack and may spread viruses through the network. Think twice before you connect that laptop to the network!



KNOW YOUR WORMS AND VIRUSES

We can no longer assume that an e-mail is legitimate just because it's from a coworker, supervisor, friend, or familiar organization. Viruses and worms routinely fake the sender's name and e-mail address to look as though the message is from someone you know and trust. The intent is to trick you into clicking on a Web link or an attachment that opens a virus or worm, allowing it to spread throughout the network. Once a worm infects your computer it can spread and infect more computers by sending itself as an e-mail attachment to anyone whose e-mail address is on your computer.



Be suspicious if:

- The subject line is blank.
- The subject line and message use bad grammar and have misspellings.
- Several messages have the same subject line.
- The subject line has odd symbols and characters in it, or is in uppercase.
- The message asks you to update or change your account.
- The message stresses urgency and immediate action.
- The message pretends to be a server-generated message (e.g., a delivery error message for an e-mail that you never sent).
- The attachment is from someone you do not know.
- The attachment has an uncommon file extension, such as .exe, .scr, or .pif.
- The attachment is described as an important software update or patch.

GOOD PASSWORD HABITS

- Immediately change any new or default password assigned to you.
- Choose passwords at least 6 characters in length with a mix of numbers and upper and lowercase letters.
- Avoid words found in any dictionary and in any language, whether spelled forwards or backwards.