

Mobile Security

Mobile computing offers the freedom of using your notebook computer or other mobile device in many remote locations. With this freedom also comes greater responsibility to keep the computer and information secure.

Securing Your Computer

Follow the steps in **8 Steps to Secure Your Computer** on the inside of this pamphlet.

Physical Security

Portable computers have an added risk of being easier to steal. It is important to have a way to secure your computer when you are not using it.



- Lock your notebook computer in a safe location when not in use.
- Buy and use a notebook security cable.

Wireless Precautions

Using WiFi is a convenient way to use the network from remote locations. However this is a shared network. A shared network is like a dinner party - anyone can eavesdrop on your conversation, if they know how.

Secure Web Browsing

Use secure, encrypted sessions using **https** for Web browsing and **SSH** instead of Telnet for logging into servers.

Secure Internet Transactions

Use UCI's **VPN** to encrypt all your network traffic.

Data Security

Under California law, California residents must be notified when a computer security breach (including loss or theft of equipment) is reasonably believed to have allowed their personal information to be acquired by an unauthorized person. UCI requires that employees take appropriate care of sensitive data that is stored on computers, PDAs or other devices. **Do not store sensitive data unless absolutely necessary.**

What is Sensitive Data?

Sensitive data is restricted data for which access or modification is limited by law or University policy. A prime example of such data (unless the data is encrypted) is an individual's first name or first initial and last name in combination with any of the following:

- Social security number
- Driver's license number or California ID card number.
- Financial account information, such as a credit card number.

Report any sensitive data stored on your computer to your Electronic Security Coordinator.

*This pamphlet outlines some basic concepts of **Safe Computing**. Detailed information and instructions can be found on the Safe Computing Website at:*

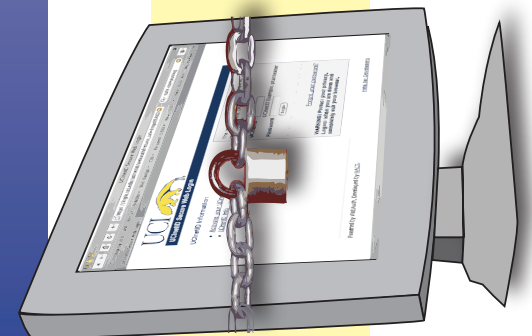
www.security.uci.edu

This information is provided by Network and Academic Computing Services (NACS) with input from Administrative Computing (Adcom), the Electronic Security Coordinators and other members of the UCI Community.

Updated – August 20, 2008

UCIrvine | Safe Computing

Simple steps you can take to protect your computer from cyber attacks.



www.security.uci.edu

8 Steps To Secure Your Computer

There are simple steps you can take to make your computer safer. Any computer connected to the network is vulnerable to attack, but by following the steps below you can minimize your risk.

Required

1. Safely Install Your Operating System

Follow the guidelines from NACS to safely install your operating system. Unprotected systems can get attacked quickly on the network.

2. Update Your Operating System

Most security issues are related to vulnerabilities in the operating system. As these flaws are discovered software companies release patches and updates to protect you from the security holes.

3. Install and Update Anti-Virus Software

One of the largest risks to a network and your data is an infected or compromised computer. Anti-virus software is critical to practice safe computing.

4. Use Strong Passwords

By default modern operating systems are accessible remotely. If you have not set a strong administrative password or left it blank, this makes your computer vulnerable to various types of attacks, including "dictionary attacks" which is a rapid, automated guessing of common passwords.

Strongly Recommended

1. Enable Firewall Protection

Firewall software can help protect your computer against hackers and other security attacks. Severe attacks can delete important information, crash your system, or steal private information like passwords or credit card numbers. Windows XP, Vista and Mac OS X (v. 10.2 or later) have built in firewalls.

2. Install and Use Spyware Removal Tools

Spyware is software that is downloaded and installed onto your computer, often without your knowledge. Spyware monitors and shares your information while you browse the Internet.

3. Back Up Important Files

No system is completely secure. If you have important files stored on your computer, copy them to another removable drive or disc and store them in a different location from your computer.

4. Enable Screen Saver Passwords

When you are away from your computer, lock the screen or set a screen saver password. This will prevent someone from using your computer when you are away from your desk.

Email Safety Tips

1. Don't Open Unexpected Attachments

Viruses are often sent via email attachments. UCI scans incoming email (sent to "@uci.edu" addresses) and cleans known viruses. However, new viruses may get through before our anti-virus software has been updated.

2. Use Spam Filters

Spam is often more of an annoyance than a security risk. However, many email viruses are sent as spam and can be caught by spam filters before they end up in your Inbox. Some phishing email messages are also caught by spam filters. UCI employs various methods to block spam from getting to you. If you use NACS Mailbox Services you can set up spam filters using "My Email Options".



3. Beware of Spoof Email or Phishing

Phishing emails are an attempt by thieves to lure you into divulging personal information for their profit. Learn to recognize the telltale signs of Phishing.

4. Don't Send Sensitive Data in Email

When you send a message, you no longer have control over what is done with it or to whom it is forwarded.