

CYBER-SAFETY BASICS

A computer security tutorial for
UC Davis students, faculty and staff



INTRODUCTION

This tutorial provides some basic information and practical suggestions for protecting your personal information and computer from cyber-attacks. Cyber-safety topics covered include:

What is Cyber-safety?

Cyber-safety threats

Consequences of inaction

Cyber-safety actions

Cyber-safety at home & work

Campus Cyber-safety services

WHAT IS CYBER-SAFETY?

- Cyber-safety is a common term used to describe a set of practices, measures and/or actions you can take to protect personal information and your computer from attacks.
- At UC Davis, we have the Cyber-safety Program policy, [PPM 310-22, UC Davis Cyber-Safety Program](#), which establishes that all devices connected to the UC Davis electronic communications network must meet certain security standards.
- As part of this policy, all campus units provide annual reports demonstrating their level of compliance.
- Further, there are services in place to help all students, faculty and staff meet the cyber-safety standards. This tutorial provides specific information about these services.



UC Davis Mrak Hall

CYBER-SAFETY THREATS

First, let's talk about some common cyber-safety threats and the problems they can cause . . .

Viruses

Viruses infect computers through email attachments and file sharing. They delete files, attack other computers, and make your computer run slowly. One infected computer can cause problems for all computers on a network.

Hackers

Hackers are people who “trespass” into your computer from a remote location. They might use your computer to send spam or viruses, host a website, or do other activities that cause computer malfunctions.

Identity thieves

These people obtain unauthorized access to your personal information, such as Social Security and financial account numbers. Then they use this information to commit crimes, such as fraud or theft.

Spyware

Spyware is software that “piggybacks” on programs you download, gathers information about your online habits, and transmits personal information without your knowledge. It might also cause a wide range of other computer malfunctions.

CONSEQUENCES OF INACTION

In addition to the risks identified on the previous slide, as part of the UC Davis community you may face a number of other consequences if you don't protect personal information and your computer. Consequences include:



Loss of access to the campus computing network



Loss of confidentiality, integrity and/or availability of valuable university information, research, and personal electronic data



Lawsuits, loss of public trust and/or grant opportunities, prosecution, internal disciplinary action, or termination of employment

CYBER-SAFETY ACTIONS

- The following slides describe the top seven actions you can take to protect personal information and your computer. These actions will help you meet the UC Davis Cyber-safety Program policy standards.
- By implementing all seven measures, you will protect yourself, others, and your computer from many common threats.
- In most cases, implementing each measure will only take a few minutes.
- You can find more about cyber-safety on the UC Davis Computer Security website, <http://security.ucdavis.edu/>

TOP SEVEN CYBER-SAFETY ACTIONS

Additional information about each of the actions below is provided on slides 8-14. Faculty and staff should work with their technical support coordinator before implementing these measures.



1. Install OS/Software Updates



2. Run Anti-virus Software



3. Prevent Identity Theft



4. Turn on Personal Firewalls



5. Avoid Spyware/Adware



6. Protect Passphrases and Passwords



7. Back up Important Files



INSTALL OS/SOFTWARE UPDATES

- Updates--sometimes called *patches*--fix problems with your operating system (OS) (Microsoft Windows, Mac OS X) and software programs (e.g., Microsoft Office applications).
- Most new operating systems download updates by default. Be sure to work with your technical support coordinator.
- To see if there are patches for your system and software, visit:
 - Windows Update: <http://windowsupdate.microsoft.com> to get or ensure you have all the latest operating system updates. Newer Windows systems are set to download these updates by default.
 - Apple: <http://www.apple.com/support>
 - Unix: Consult documentation or online help for system update information and instructions.



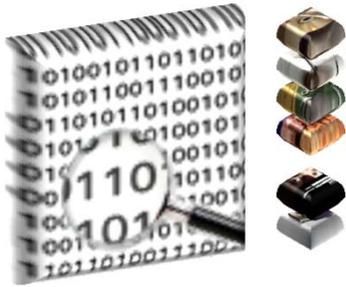
RUN ANTI-VIRUS SOFTWARE

- UC Davis requires each computer that connects to the campus network from home or work be protected by anti-virus (AV) software.
- Installing and running an anti-virus program avoids computer problems caused by viruses. Be sure to work with your technical support coordinator.
- Anti-virus software removes viruses, quarantines and repairs infected files, and can help prevent future viruses.
- Periodically, check to see if your anti-virus is up to date by opening your anti-virus program and checking the *Last updated:* date.
- For more information on anti-virus options, see UC Davis Software License Coordination's [FAQ for Campus Anti-Virus Software](#).



TURN ON PERSONAL FIREWALLS

- Work with your technical support coordinator to check your computer's security settings for a built-in personal firewall.
- Microsoft Windows and Mac OSX have built-in firewalls. See:
 - Mac <http://support.apple.com/kb/HT5413>
 - Microsoft <http://windows.microsoft.com/en-us/windows-8/windows-firewall-from-start-to-finish>
 - Unix users should consult system documentation or online help for personal firewall instructions and/or recommendations.
- Once your firewall is turned on, have your technical support coordinator test your firewall for open ports that could allow in viruses and hackers. Firewall scanners like the one on <http://www.auditmypc.com/firewall-test.asp> simplify this process.
- Firewalls act as protective barriers between computers and the Internet.
- Hackers search the Internet by sending out pings (calls) to random computers and wait for responses. Firewalls prevent your computer from responding to these calls.



AVOID SPYWARE/ADWARE

- Spyware and adware take up memory and can slow down your computer or cause other problems. Tools to remove spyware/adware are available. Work with your technical support coordinator.
- Spybot and Ad-Aware to remove spyware/adware from your computer are available to UC Davis students, faculty and staff for personal use for free from the UC Davis Software License Coordination website, <http://software.ucdavis.edu>
- Watch for allusions to spyware and adware in user agreements, before you install free software programs.
- Be wary of invitations to download software from unknown Internet sources.



BACK UP IMPORTANT FILES

- Reduce your risk of losing important files to a virus, computer crash, theft or disaster by creating back-up copies.
- Keep your critical files in one place on your computer's hard drive so you can easily create a back-up copy.
- Save copies of your important documents and files to a CD, online back-up service, flash or USB drive, or a server.
- Store your back-up media in a secure place away from your computer, in case of fire or theft.
- Test your back-up media periodically, to make sure you can access and read the files.



PREVENT IDENTITY THEFT

- Don't give out financial account numbers, Social Security numbers, driver's license numbers or other personal identity information unless you know exactly who's receiving it. Protect others people's information as you would your own.
- Never send personal or confidential information via email or instant messages. They can be easily intercepted.
- Beware of phishing scams. They are frauds that use email messages that appear to be from a reputable business (often a financial institution) in an attempt to gain personal or account information. Never enter personal information into an online form you accessed via a link in an email you were not expecting to receive. Legitimate businesses will not ask for personal information online.
- Order a copy of your credit report from each of the three major credit bureaus: Equifax, Experian, and Trans Union. Reports can be ordered online at each bureau's website. Make sure reports are accurate and include only those activities you have authorized.



PROTECT PASSPHRASES AND PASSWORDS

- Do not share your passphrase, and always make it difficult to guess by mixing letters, numbers and punctuation, and avoid using dictionary words.
- Do not use one of these common passphrases or any variation of them: qwerty1, abc123, letmein, password1, iloveyou1, (yourname1), baseball1.
- Change your passphrase periodically.
- When choosing a passphrase:
 - Use a mix of at least three of the four character types (upper case, lower case, symbol or number)
 - Don't use more than 10 characters of any one type (no more than 10 numerals or letters).
 - Avoid the use your birthdate, login account or first or last name in the passphrase
- Store a passphrase or passwords in a safe place. Consider using KeePass Password Safe (<http://keepass.info/>), Keychain (Mac) or an encrypted USB drive to store passwords. Avoid keeping a passphrase or passwords on a Post-it under your keyboard, on your monitor, or in a drawer near your computer!

CYBER-SAFETY AT HOME

- Physically secure your computer with security cables. Lock doors and windows in the dorms and off-campus housing.
- Avoid leaving your laptop unsupervised and in plain view in the library or coffee house, or in your car, dorm room or home.
- Set up a user account and password to prevent unauthorized access to your computer files.
- Do not install unnecessary programs on your computer.
- Microsoft users can download the free Secunia Personal Software Inspector (<https://psi.secunia.com/>), which lets you scan your computer for any missing operating system or software patches, and provides instructions for getting all the latest updates.

CYBER-SAFETY AT WORK

- Work with your technical support coordinator before implementing new cyber-safety measures.
- Talk with your technical support coordinator about what cyber-safety measures are in place in your department.
- Report to your supervisor any cyber-safety policy violations, security flaws/weaknesses you discover, or any suspicious activity by unauthorized individuals in your work area.
- Physically secure your computer by using security cables and locking building or office doors and windows.
- Do not install unnecessary programs on your work computer.



CAMPUS CYBER-SAFETY SERVICES

UC Davis offers services and software to protect the campus network against cyber-safety attacks. These include:

Services	Software
<ul style="list-style-type: none">▪ Campus email virus filtering▪ Campus firewall services▪ Email attachment filtering▪ Vulnerability scanning▪ Intrusion prevention system	<ul style="list-style-type: none">▪ Free change management software: Tripwire▪ Free Spyware/adware removal tools for personal use

For more about these and other campus cyber-safety services, visit <http://security.ucdavis.edu>

QUESTIONS?

- For more information about cyber-safety at UC Davis, visit <http://security.ucdavis.edu>.
- For answers to questions about this tutorial, contact cybersecurity@ucdavis.edu.
- For help implementing a cyber-safety measure on your work/school computer, contact IT Express at (530) 754-4357.

CYBER-SAFETY BASICS QUICK QUIZ

1. True or False? Viruses can be transmitted via email, email attachments or IM.
2. People who seek out your personal information and then use it to commit crimes are called:_____
3. Which of these methods help prevent identity theft? (Check all that apply.)
 - A. Never send personal information via email or instant messages.
 - B. Always send personal information via email or instant messages.
 - C. Lock my office door.
 - D. Don't tell anybody my name.
4. True or False? Iloveyou2 is a good passphrase. Why or why not?
5. I just downloaded a free program online and now my computer is running very, very slowly. Which of the following most likely happened?
 - A. I didn't install the program properly.
 - B. I didn't have enough space on my hard drive for the new program.
 - C. I downloaded spyware and/or adware, too.
 - D. Someone snuck in while the program was downloading and changed my password.
6. _____help prevent your computer from responding to pings (calls) from hackers.
7. To fix problems with my operating system and/or application software, I should install _____.

Answers on next slide . . .

QUICK QUIZ ANSWERS

1. True
2. Identity thieves
3. A and C are correct. D would probably help too, but seems a bit extreme!
4. False. Iloveyou2 is a very common passphrase.
5. C. It's most likely that you downloaded spyware and/or adware.
6. Firewalls
7. OS and/or software updates (patches)



How did you do?

7-6 correct: Fantastic!

5-4 correct: Good.

3-1 correct: You might want to review the material for the questions you missed.

REFERENCES

- UC Davis Cyber-safety Program policy (see PPM 310-22)
<http://manuals.ucdavis.edu/PPM/contents.htm>
- UC Davis Cyber-safety Program
<http://security.ucdavis.edu/cybersafety.html>
- UC Davis Security website
<http://security.ucdavis.edu>
- Cyber-Safety Basics
<http://security.ucdavis.edu/cybersafetybasics.html>

CREDITS

The Cyber-safety Basics tutorial is provided by:

UCDAVIS

**INFORMATION AND
EDUCATIONAL TECHNOLOGY**