CYBER-SAFETY BASICS

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






UC DAVIS INFORMATION & EDUCATIONAL TECHNOLOGY

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...

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, (http://manuals.ucdavis.edu/ppm/310/310-22.htm) 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. Specific information about these services is provided in this tutorial.

UC Davis Mrak Hall

Threats

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 may use your computer to send spam or viruses, host a Web site, or do other activities that cause computer malfunctions.

Identity Thieves

People who obtain unauthorized access to your personal information, such as Social Security and financial account numbers. They then 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 may also cause a wide range of other computer malfunctions.

Consequences

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 fail to take actions to 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/or personal electronic data

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

Actions

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 of these security measures, you will protect yourself, others, and your computer from many common threats.
- In most cases, implementing each of these security measures will only take a few minutes.
- You can find more about cyber-safety on the UC Davis Computer Security Web site (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 Passwords

7. Back up Important Files

Install OS/Software Updates

- Updates-sometimes called *patches*-fix problems with your operating system (OS) (e.g., Windows XP, Windows Vista, Mac OS X) and software programs (e.g., Microsoft Office applications).
- Most new operating systems are set to download updates by default. After updates are downloaded, you will be asked to install them. Click yes!
- To download 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 only. Newer Windows systems are set to download these updates by default.
  - Microsoft Update: http://www.update.microsoft.com/microsoftupdate/ to get or ensure you have all the latest OS **and** Microsoft Office software updates. You must sign up for this service.
  - Apple: http://www.apple.com/support
  - Unix: Consult documentation or online help for system update information and instructions.
- Be sure to restart your computer after updates are installed so that the patches can be applied immediately.

Run Anti-Virus Software

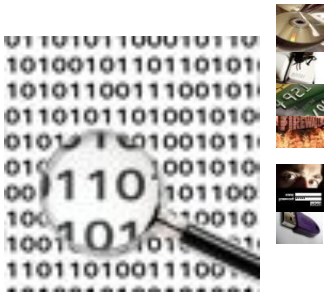
- To avoid computer problems caused by viruses, install and run an anti-virus program like Sophos.
- Periodically, check to see if your anti-virus is up to date by opening your anti-virus program and checking the *Last updated:* date.
- Anti-virus software removes viruses, quarantines and repairs infected files, and can help prevent future viruses.
- UC Davis students, faculty and staff can get Sophos for their work and home computer for FREE on the Internet Tools CD (available from IT Express in Shields Library).
- Sophos can also be downloaded for free from the UC Davis Software License Coordination Web site (https://my.ucdavis.edu/software/).

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 as these can be easily intercepted.
- Beware of phishing scams - a form of fraud that uses email messages that appear to be from a reputable business (often a financial institution) in an attempt to gain personal or account information. These often do not include a personal salutation. Never enter personal information into an online form you accessed via a link in an email you were not expecting. 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 of the bureaus' Web sites. Make sure reports are accurate and include only those activities you have authorized.

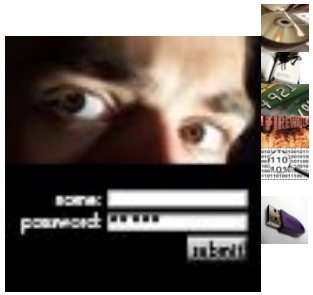
Turn on Personal Firewalls

- Check your computer's security settings for a built-in personal firewall. If you have one, turn it on. Microsoft Vista and Mac OSX have built-in firewalls. For more information, see:
  - Mac Firewall (docs.info.apple.com/article.html?path=Mac/10.4/en/mh1042.html)
  - Microsoft Firewall (www.microsoft.com/windowsxp/using/networking/security/winfirewall.mspx)
  - Unix users should consult system documentation or online help for personal firewall instructions and/or recommendations.
- Once your firewall is turned on, 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.
- Use Spybot and Ad-Aware to remove spyware/adware from your computer. UC Davis students, faculty and staff can get Spybot and Ad-Aware for free on the Internet Tools CD (available from IT Express in Shields Library).
- Watch for allusions to spyware and adware in user agreements before installing free software programs.
- Be wary of invitations to download software from unknown internet sources.



Protect Passwords

- Do not share your passwords, and always make new passwords difficult to guess by avoiding dictionary words, and mixing letters, numbers and punctuation.
- Do not use one of these common passwords or any variation of them: qwerty1, abc123, letmein, password1, iloveyou1, (yourname1), baseball1.
- Change your passwords periodically.
- When choosing a password:
  - Mix upper and lower case letters
  - Use a minimum of 8 characters
  - Use mnemonics to help you remember a difficult password
- Store 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 passwords on a Post-it under your keyboard, on your monitor or in a drawer near your computer!

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 the files are accessible and readable.

Home

CYBER-SAFETY AT HOME

- Physically secure your computer by using security cables and locking 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.

Work

CYBER-SAFETY AT WORK

- Be sure to 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/office doors and windows.
- Do not install unnecessary programs on your work computer.

Campus Services

CAMPUS CYBER-SAFETY SERVICES

UC Davis offers services and software to protect the campus network

against cyber-safety attacks. These include:

Services	Software
▪Campus email virus filtering ▪Campus firewall services ▪Email attachment filtering ▪Vulnerability scanning ▪Intrusion prevention system	▪ Free anti-virus software: Sophos Anti-virus ▪ Free encryption software: Pointsec for PC ▪ Free change management software: Tripwire

Additional information 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 itsecurity@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.

1. People who seek out your personal information and then use it to commit crimes are called:_____

1. Which of the following are ways to 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.

2. True or False? Iloveyou2 is a good password. Why or why not?

1. Which anti-virus program is available to all UC Davis students, faculty and staff for free?_____

1. 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.

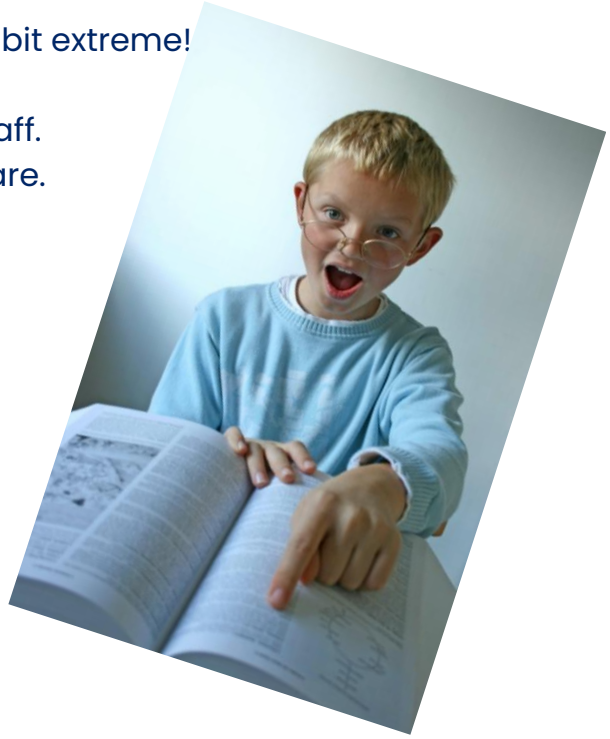
2. _____help prevent your computer from responding to pings (calls) from hackers.

8. 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 password.
5. Sophos Anti-Virus is free to UC Davis students, faculty and staff.
6. C. It's most likely that you downloaded spyware and/or adware.
7. Firewalls
8. OS and/or software updates (patches)



How did you do?

8-7 correct: Fantastic! You can help write the next quiz!
6-5 correct: Good. You can help write the next quiz, but we'll check it for accuracy . . . just in case.
4-3 correct: You might want to review the material for the questions you missed.

ONE MORE THING . . .

We want to hear from you! Send stories about your cyber-safety experience, or suggestions for additional information that we should include in this tutorial or on the
security Web site, to Julie McCall at itsecurity@ucdavis.edu.

Thank you!

REFERENCES

- UC Davis Cyber-safety Program policy (PPM 310-22) (http://manuals.ucdavis.edu/ppm/310/310-22.htm)
- UC Davis Cyber-safety Program (http://security.ucdavis.edu/cybersafety.cfm)
- UC Davis Security Web Site (http://security.ucdavis.edu)
- Cyber-Safety Basics (http://security.ucdavis.edu/cybersafetybasics.cfm)

CREDITS

The Cyber-safety Basics tutorial is provided by:

UC DAVIS INFORMATION & EDUCATIONAL TECHNOLOGY

Content by Bob Ono and Julie McCall
Design and layout by Julie McCall