CYBER-SAFETY

Rushikesh D. Bulbule

Department of Computer Science and Engineering, SVERI's College of Engineering, Pandharpur

Third Year Engineering Student

CYBER-SAFETY BASICS:

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.

As part of this policy, all campus units provide annual reports demonstrating their level of compliance. 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 manual.

CYBER THREADS

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. 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.

TOP 7 ACTIONS TAKEN BY THE CYBER SATFY

INTALL OS/SOFTWARE

- 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.

CAMPUS CYBER-SAFETY SERVICES

Campus email virus filtering

Campus firewall services

Email attachment filtering

Vulnerability scanning

Intrusion prevention system