



Helpful Desktop Computing Security Basics at Fairfield University

1 – Develop and maintain strong passwords.

Passwords should be at least eight characters (using letters and numbers) in length and should not contain whole English words. **Do not use personal information** (social security #, names, birthdays, addresses, phone #'s etc.) Instead, use acronyms or abbreviations of long phrases.

- Good Password Example (abbreviation style): I!2uzC@W (I love to use computers at work)
- Bad Password Example: dellcomputer

Change your password often. Fairfield University has a mandatory 3 month password reset policy. Please go to the following website for automatic password reset information: www.fairfield.edu/passwords.

2 – Do not share your passwords with anyone.

A common practice for many institutions is for people to simply share passwords for convenience. This is perhaps the easiest way for someone to gain access to information on your computer or the systems you log into (Banner, StagWeb, Outlook E-Mail, your computer etc.) **You should NEVER tell anyone your password** and you should also refrain from writing down your password especially in a place where someone might look for it (on your monitor, under your keyboard, in your desk). If your password is stolen and someone uses it to do harm, it will appear as though you were the one that did it.

For more information about password security, please go to the C&NS training website for documentation on “Tips for creating safe passwords and account security” located at: www.fairfield.edu/x14070.xml

3 – Backup your data regularly.

Documents on your computer are not automatically backed up or saved to a remote space for safety and security purposes. All users should take the time to backup their data (especially sensitive data) using a CD, floppy/Zip disk or USB key. Also make sure these media are stored in a safe place. Files on your computer can be automatically backed up to the Artemis server for your convenience. Please call the C&NS helpdesk at x4069 for more information.

4 – Save your work frequently and to multiple sources.

If you are working in a program and the power goes out, you will lose all information from your last save. **You should save all your work frequently. More importantly, you should save your work/document as soon as you begin.** This will ensure that you have at least something saved if something inconvenient happens. As a tip, Microsoft Office programs can auto-save documents for you, but you must initially save your document. Usually, this setting is turned on by default. There is also the reality that your hard drive may develop problems. To avoid data inconveniences, copy or backup your data as described in topic number 3. For more information about saving and auto-saving, please contact the C&NS helpdesk at x4069.

5 – Physically secure your computer.

The best way to protect your data is by physically securing the computer that your data resides on. **1.** Always lock your office door (if you have one) at the end of the day and when you leave your desk. **2.** Make sure that you either log off your computer or lock your computer desktop when away from your desk. Locking a computer's desktop allows someone to password protect their computer without logging off or shutting the computer down. This can be done on Windows XP machines by simply pressing the Windows Key and the letter 'L' at the same time. Unlocking your computer requires you to enter your network username and password. (On a Mac, "fast user switching" must be turned on) **3.** Physically lock down your computer with a cable lock or other locking mechanism with a key or combination helps to prevent theft. For questions concerning the physical security of your computer, please contact the C&NS helpdesk at x4069.

6 – Never install illegal or un-licensed software on your machine.

There are a number of free applications to download and install from the Internet. However, some software is written to steal your data. Also, some software can actually be viruses, many of which are distributed via peer-to-peer file sharing programs like Limewire, KaZaA or Gnutella. **Software should only be installed by Computing and Network Services staff.** If you want something installed for work-related reasons, we can schedule an appointment with you to get this done. For more information about viruses, spyware, phishing and spam, please go to the following C&NS training website for documentation on "Internet Annoyances: Viruses, Spyware, Spam and Phishing": <http://www.fairfield.edu/x14073.xml>.

7 – Be wary of wireless internet access (Especially at home!)

Most people think wireless network connections are a wonderful convenience, but wireless transmissions can be easily intercepted and passwords can be hacked by someone who knows what they are doing. **Never use a wireless connection when a hard-wired option is available.** If you must use wireless, then make sure that you do not use critical applications that hold sensitive data so that you minimize the risk of data loss or security breaches. For instructions to connecting to wireless networks on campus, please go to the following website for documentation under the heading "Connecting to Classroom Wireless Networks": <http://www.fairfield.edu/x14070.xml>.

8 – Email Wisely

Never send an email that you wouldn't want everyone on campus to see. If someone gets an email that they shouldn't have received, you may see that email come back to haunt you. Confidential documents should be hand-delivered to ensure that nobody, other than their intended recipient reads them.

Many companies scan emails coming in and going out of their servers for appropriate content. Fairfield University does not do this, but please use your own personal (non-Fairfield University) email account like AOL, Yahoo, HotMail, or Google to send personal emails. This will also limit the amount of spam emails you receive in your Outlook account.

Never open suspicious attachments. Most unwanted attachments contain viruses that can wreak havoc on your computer. If you are suspicious of an e-mail, don't even open it let alone open the attachment. Just delete it. If it is legitimate or important enough, the sender will send it to you again. For questions concerning e-mail security, please contact the C&NS helpdesk at x4069.

9 – Password-protect your files.

Microsoft Office and other applications allow for people to password protect their files thus preventing others from reading them or altering them. In Microsoft Office on the PC, go to Tools>Options and click the Security tab and you will find an easy way to password protect your document. (For the Mac, go to Word>Preferences>Security) For any questions about document security, contact the C&NS helpdesk at x4069.

10 – Don't have a shredder? Get one.

There are reams of paper that get thrown out every day. An enterprising snoop may well decide to check the trash to see what they can find. Some data that is very sensitive has been recovered from Fairfield University trash bins in the past. **Shredding paper documents that contain personal or sensitive data is a must.** If you toss it in the trash, you are only asking for trouble. For purchasing appliances of this nature, please contact the Purchasing department at x2205.

11 – Call C&NS for help.

If you think your machine has been compromised or if you have any questions concerning computer security, please call us immediately. **We can help.**

Contact Information:

Location – Dolan Commons, 2nd floor

Telephone - x4069

E-mail – cns@mail.fairfield.edu