Laptops and Security

Written by
Information Services
North Orange County Community College District

Table of Contents

Overview

Security... hardly a day goes by when we don't hear the term used in one way or another. Security can refer to personal security, data security, physical security, etc., etc!. Of course, here, we are referring to laptop security - both physical security as well as securing the data held within the laptop.

In the past data was stored only at the work place; the data never left the building. But now we live in a very mobile society. We are on the move - so we require the data to be on the move with us! This new mobility, although wonderfully convenient, has opened another door... an unsecure door. You hear it all the time:

- *"Colleges across the country, through computer security failure and human error, have exposed confidential information about hundreds of thousands of students and employees over the Internet, and experts say they expect the problems to continue. In addition to being targeted by some very savvy hackers, college computer systems have been made vulnerable by the schools themselves through inadequately trained employees who have access to the files."*
  http://www.sfgate.com/cgi-bin/article.cgi?file=/c/a/2004/04/05/MNGGP60LNV1.DTL

- *"UCLA is alerting approximately 800,000 people that their names and certain personal information are contained in a restricted database that was illegally and fraudulently accessed by a sophisticated computer hacker. "*
  http://newsroom.ucla.edu/page.asp?RelNum=7571

- *"In what could be the largest data security breach to date, MasterCard International on Friday said information on more than 40 million credit cards may have been stolen."*
  http://news.com.com/MasterCard+breach+hits+40+million+accounts/2100-1029_3-5751886.html

and the list goes on and on.

So what is one to do? There are several things one can do to minimize the risk of a security breach. These include:

- **Know your laptop**. Know the components, where is data stored, how you connect to the Internet, etc.
- **Know your data**. What data is considered confidential? What kind of information do you store on your laptop? Where do you store your data? Do you backup your data on a regular basis? Where do you store your backup copy?
- **Physical security**. What can you do to prevent your laptop itself from being compromised or stolen?
- **Data security**. What can you do to protect confidential data itself? This can include things such as password protection, encryption, etc.

This document has been written to help you learn how to protect your laptop and the data you store on it. Understanding your data and the various methods of protecting it is half the battle. When it comes down to it, it is you - the laptop owner that is responsible. The responsibility of protecting your laptop and it's data lies with you. We will give you the knowledge and tools

needed to protect your laptop and data within, but you must be an active participant! Thieves get smarter and smarter all of the time. So, we, too, must be "smart" and strive to stay one step ahead of them.

Know Your Laptop

Your laptop can consist of various components, both internal and external. Your laptop, of course, has a hard drive, keyboard and monitor all built into a nice, tiny package. But you may have other components, such as, but not limited to, a battery, docking station, external mouse, CD or DVD device, thumb (flash) drive, etc. This section will help to familiarize you with the components that you have.

My Laptop Information

Use this section to write down information about your laptop:

Make and Model: _____

Serial Number: _____

Date Received: _____

District Barcode: _____

Basic Components

Use this section to write down what kind of components you have or use regularly.

Hard Drive size:
Will you be using any external storage? (flash drive, CD, DVD, etc.)
Battery/ battery life:
USB ports (if yes, how many?):
Universal Security Slot:
Screen Resolution: *NOTE: Screen Resolution must be set at 1024x768 if using Banner.*

Other things I attach or plug into my laptop?:

Connecting to the Internet

There are many ways to connect to the Internet. At the campuses, connection to the Internet is provided through CENIC, the education network for the State of California. We protect our internal network from the Internet with a firewall at each of our connection points to the Internet. We protect our applications and data by requiring authorized userids and passwords for staff.

Our desktop systems require a person to sign on with a userid and password. That same authentication allows a person to use other networked services such as GroupWise, Outlook, etc.

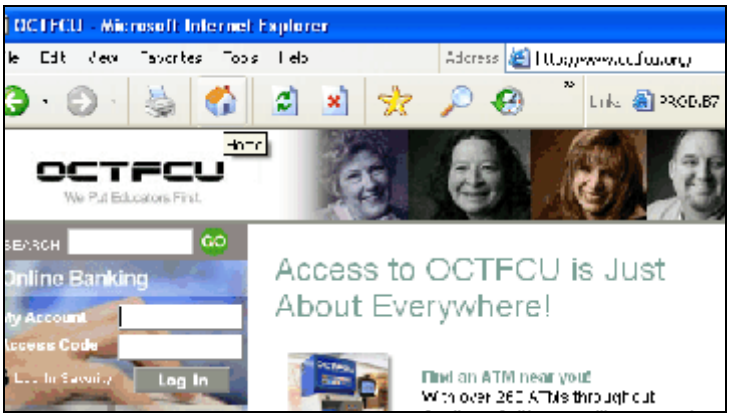
Outside of the workplace, there are various ways to connect to the Internet: broadband cards, air cards, wireless networks, DSL, cable modem, phone modem, etc. Some of this access is secure and some of it is not. When you connect to the Internet at work, you are in a secure environment. The colleges have many layers of protection, including (but not limited to) firewalls, network accounts, and password protection. When you connect outside of work, whether it be at your home, a hotel, or the local coffee shop, you need to be aware that these environments are usually not protected like they are at the work place.

What you need to connect to when you are away from the campus will determine what security you may need to use to ensure a secure environment. If you need to connect to your e-mail, you will probably use a web access version of your e-mail program. This does not require extra security. If you are connecting to Banner, you must use Virtual Private Network (VPN) in order to do so. This does require additional security, including a userid and password for the VPN access.

Secure vs. Unsecure Connections

A secure wireless connection is one that uses encryption to secure communication. Sending sensitive information over the Internet from a secured wireless connection provides added security to that information. An unsecure wireless connection has no encryption and the information sent is in a format call “clear text”; anyone intercepting the transmission can read the data.

There are two general indications of a secured web page:



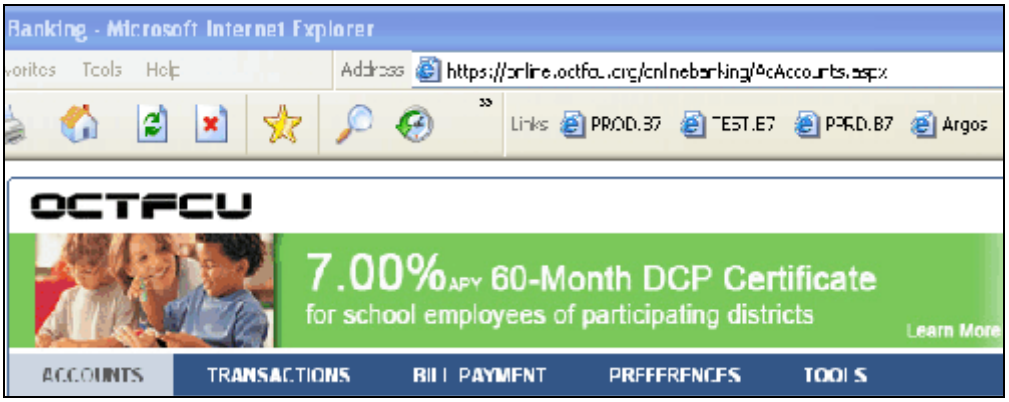
Check the web page URL

Normally, when browsing the web, the URLs (web page addresses) begin with the letters “http”. When the connection is a secure connection, the web address displayed should begin with “**http**” - note

the

For example, http://www.octfcu.org This URL takes you to the Credit Union's home page. It is *not* a secure page.

When I enter in my asterid, password and click on log in, I am taken to a secure web page. Notice the URL now shows "**https**". This tells you the account number and access code will be encrypted before it is sent.



Check for the "lock" icon

There is a general standard to display a "lock" icon, usually in the lower right of the browser window. The lock is not just a picture. You can click (or double click) on it to see details about the web site's security.

Know Your Data

Step one in keeping data secure is knowing what *kind* of data is kept on your laptop. Data files can be created in any program (Word, Excel, Access, etc). Data files can have information that is considered confidential in it. You may have data files that you consider important, but it doesn't have confidential information in it. Do you have research information on your laptop? What is considered confidential? Etc. You can see that understanding your data and what data is confidential is a very important first step!

FERPA

What is FERPA? FERPA is the **F**amily **E**ducation **R**ights and **P**rivacy **A**ct. It is a federal law that protects the privacy of student education records. It basically tells us what we can and cannot do with student information. For more information about FERPA, you can visit their web page at: http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html

FERPA states that institutions can give out directory information *without* the consent of the student. FERPA defines **directory information** of name, address, phone number, date and place of birth, honors and awards, and dates of attendance. However, the NOCCCD Board of Trustees have further defined what we, NOCCCD, can give out as directory information in **Board Policy 5040, section 5.0**. This policy states that the *only* information we can give out without

student consent is:

- Student participation in officially recognized activities and sports including weight, height and high school of graduation of athletic team members.
- Degrees and awards received by students, including honors, scholarship awards, athletic awards and Dean's List recognition.
- See http://www.nocccd.edu/Policies/PDFs/5040.BP_062005.pdf
- You may also see California Civil Code 1798.29, which talks about personal information. http://www.privacy.ca.gov/code/ipa.htm

What does this all mean to you?

If you have a **Banner or Argos login**, you have access to information that is considered confidential. That means that your access is just that... confidential. Ask yourself these questions:

Do I, at times use someone else's username to access Banner?
Do I allow others to use my Banner username and password?

Remember:

***NEVER use anybody else's username or password!** This is against NOCCCD policy. If your supervisor will be out of the office for an extended period of time, and you need more access rights to Banner, call the Help Desk at 84849. With the proper approvals, changes can be made to your Banner security on a temporary basis. **DO NOT use your supervisor's username and password.**

***NEVER loan out your username and password!** If someone else uses your username and password and violates FERPA, you can be held accountable.

Under the law, **an individual can be held responsible for FERPA violations**, not just the institution.

What is Confidential Data?

We all have data on our computers that we consider important. This can include e-mail, various files, presentations, etc. Even though the files are important to us, it doesn't necessarily mean they contain confidential information. Although the term "confidential information" is not one that is legally defined, it is generally understood to include any information that is held in confidence, and if disclosed, could be harmful to the individual. A variety of different kinds of information may constitute confidential information, such as software programs, business plans, personnel information, financial statements, medical information, etc. When in doubt, it is best to assume that your information is confidential and take all precautions to protect it.

Here at the Campuses, confidential information may include, but is not limited to, an individual's name and any combination of any of the following elements:

- Social Security Number
- Banner ID number
- Grades

- Personnel information
- Medical information
- Payroll information
- Banking information, including account numbers, credit card or debit numbers

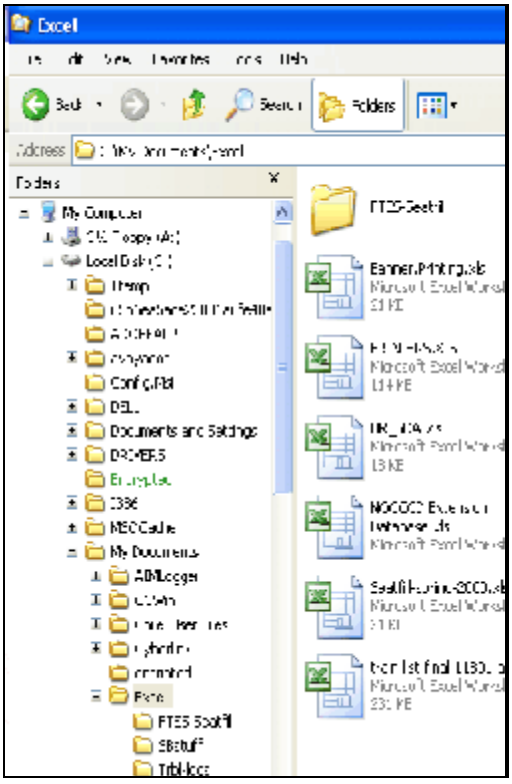
If you have any confidential information on your laptop or PC, you need to take extra precautions to ensure that the data is properly protected. These precautions can include various passwords, file protection, file encryption, and possibly entire disk encryption. District I.S. or your campus Academic Computing Technologies (ACT) department can assist you in determining which method is best for your needs.

Know Where Your Data Is Stored

Everyone has various software packages loaded on their laptops, such as Word, Excel, Outlook, GroupWise, etc. Remember that software is easy to reload easily enough should the need arise. However, you should backup the data files that you create. The first step in this process is knowing *where* those files are stored! This means that you need to understand the file structure on your PC and/or laptop.

Think of your laptop hard drive as a huge filing cabinet. This filing cabinet has many drawers. Within each of these drawers, there are many hanging folders. Within the hanging folder, there are many separate documents relating to the same subject. Your hard drive, or the "C" drive, is set up much the same way:

- Your hard drive is the huge filing cabinet named **"C"**.
- Each drawer is given a unique name - these are the main folders, such as "**My Documents**".
- Within the main folder (drawer) called "My Documents" are separate hanging folders (sub-folders).
- Within these sub-folders are several **individual documents** relating to the same subject.



Windows Explorer is a great tool for managing files on your hard drive. Using Windows Explorer, you can see exactly how your hard drive is set up and where your data is stored.

For example, using Windows Explorer, I can see my main disk drive, **"C"**.

Within my **"C"** drive, I can see that I have several folders (my drawers) which keep things nicely organized. I can see the folder called **"My Documents"**. This is where I save all of my data.

Within **"My Documents"** I have many sub-folders. One of the folders is named **"Excel"**. Within that folder I have more folders to keep everything organized. Within those folders are individual files.

Understanding the way your hard drive is structured or set up is important so that you know *where* your data is! And knowing where your data is will make it easier to backup and protect your files. Using Windows Explorer you can do many simple tasks, such as creating new folders, copying or moving files from one folder to another, copying files to a CD for backup purposes, etc.

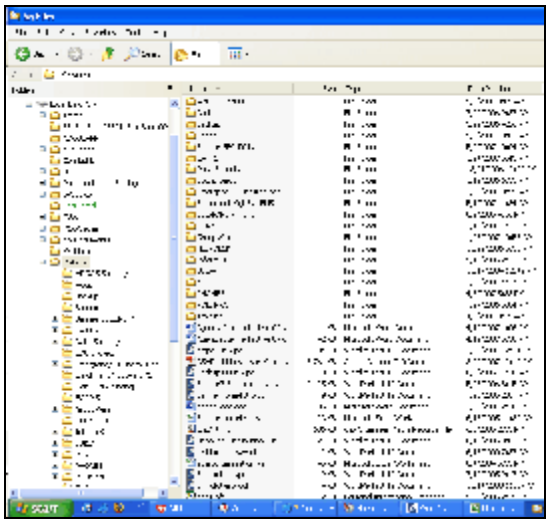
Where is My Default Location?

Every software program (Word, Excel, Word Perfect, Outlook, GroupWise, etc.) will save files to a default location. If you are not sure where this location is, you can find out by opening the program and looking at file options. For example, with Word open, click on Tools, and then Options. Once Options is open, there is a tab for File Locations. It lists all the default locations for various file types. Word documents are automatically saved to C:\My Documents.

Once you know the default locations of where your data is stored, you will also know what files or folders will need to be backed up and protected if necessary.

Backup Your Data

Knowing where your data is located is the first step. Now you need to back the information up! This is very easy using Windows Explorer. You can copy files to many different mediums, including a CD, writeable DVD, flash drive (also called a thumb drive), etc. It all depends on what components your laptop has. Most laptops have a CD drive, so we will walk through backing up files to a CD.

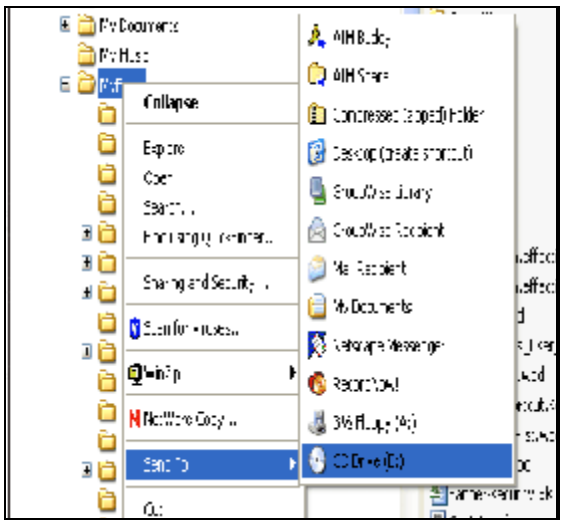


- Open Windows Explorer by clicking "Start" (green button at the bottom left corner of your screen), Programs, Accessories, Windows Explorer. (Shortcut: try right clicking on the "Start" button and selecting "Explore.")

- Once Windows Explorer is open, you will see 2 window "panes". The **left pane is the file structure**. The **right side shows you details**, or files within the folder that is highlighted in the left pane.

- Click ONE time on the folder that you would like to copy (clicking one time will highlight a

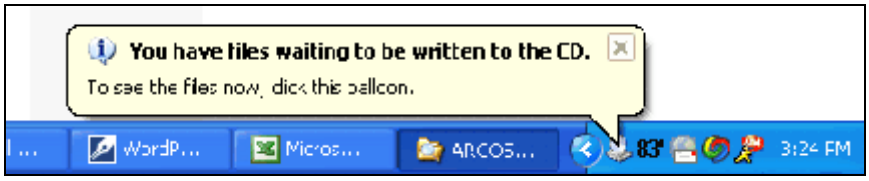
folder, clicking two times will open it).



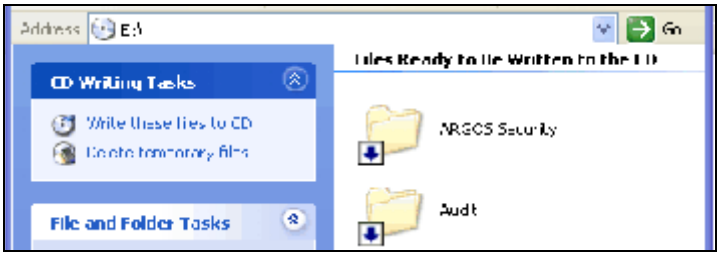
- With the folder highlighted, point to it with your mouse, RIGHT click and select (left click) “SEND TO”.
- “Send To” then gives you a list of options as to where you would like to send the file. Select your CD drive.

* In the example, I have selected a folder and want to *SEND TO* (copy the contents of that folder) to my CD drive, which is called “CD Drive (E:).

- This will send a copy of that folder and all of its contents to the CD drive. You can continue to select other folders as needed.
- On your task bar a little pop up will say “You have files waiting to be written to the CD”.



- Click on the little icon that it points to and a dialogue box will open. Insert a CD in the CD drive.
- Click on “Write these files to CD” and follow the rest of the prompts.



NOTE: If you have information that contains confidential data, you will want to take extra precautions when backing up this data. There are many software packages available to you. You may want to consider having the data encrypted on your hard drive as well as the backup itself. Please work with your Academic Computing Technologies department or District IS if this is something that you need.

Storing Your Backup Data

Making backups of your data is very important. Computer hard drives can fail, and sometimes data is unrecoverable. This can be very important, especially for laptops, as laptops are mobile and accidents can happen (a dropped laptop, stolen laptop, etc). **However, it is important to remember the CD backup you just made can be vulnerable! If you have confidential data on the CD, make sure to store the CD in a safe and secure place.** Don’t store the CD backup with the laptop. You can also encrypt the data before backing it up!

Schedule Your Backup

Come up with a backup schedule and stick to it. An easy schedule is monthly. Pick a day that is generally good for you, for example, the first Friday of every month. If you have a hard time remembering, set up a meeting in your calendar. Most calendars have reminders as well! If a problem appears and you need to restore a file, you will often hear "Oh no! I haven't done a backup since...." You will never hear someone say "Oh darn! I just backed up my laptop yesterday!"

Backup Software

There are several backup software packages on the market. Some packages will compress files, some may even automatically encrypt data. The District does not have a specific backup software package that it recommends using. If you are interested in a software package, or have the need for extra protection of your backup data, please work with your Campus Academic Computing department or District IS.

Securing Your Laptop

When one talks about laptop security, there are two main topics that immediately come to mind: *physical security* of the laptop and *data security* of the information held within the laptop. A few interesting facts:

- According to the FBI, losses due to laptop theft totaled more than $6.7 million dollars in 2005! Can you imagine what it is today?
- For the last 7 years, laptop theft has been found to cause the second highest amount of financial loss, second only to damage caused by viruses. (2005 FBI Computer Crime Survey)
- The FBI reports that only 2-3% of stolen laptops are ever recovered.
- According to the Gartner Group, 10-15% of laptops thefts are committed to obtain confidential data.
- According to a survey conducted by Kensington, 2 out of every 5 laptop thefts occur from the office!
- Gartner Group reports that the chances of a laptop being stolen are 1 in 10!

Physical Security

There are many things that one can do to help prevent the laptop itself from being stolen. Some things are very simple and low cost. Others, of course, can get more complicated and expensive. A lot will depend on the data that you store! If you do *not* store confidential information on your laptop, the simple, low cost preventions may work great for you. But if you keep confidential

information that, if stolen, could be harmful to individuals, such as name and SSN, or proprietary information that could harm the college, you may want to look into more aggressive ways of securing your laptop.

An Easy Target

Just like securing your home or car, nothing is full proof. But any measures are better than no measures at all! A thief is going to look for the easy target. If your home has an alarm system and the house next door doesn't, a thief will take the easy route! The same thing applies to your laptop. If your laptop is protected, even with something as simple as a cable lock, and the laptop next to you isn't - well, we can guess which laptop will have a higher chance of being stolen.

Another common mistake is thinking that it won't happen to you! We all think of certain places as being safe, like our home or workplace. Last year (2006), while a doctor and her family were asleep, someone broke into her house. Among the items stolen was her laptop. It was sitting there on her desk - unprotected. It was an easy target. The laptop was never recovered and she lost important research data that could not be replaced! Had the computer been locked to an immobile device (such as a desk) with a cable lock, the laptop may not have been stolen.

In this section we will address simple to aggressive measures for protecting your laptop.

Register The Laptop With The Manufacturer

Registering your laptop with the manufacturer will "flag" it if a thief ever sends it in for maintenance. It also pays to write down the manufacturer, serial number, when the laptop was acquired and store the information in a safe place. In the event your laptop is stolen, it will be impossible for the police to ever recover it if they can't trace it back to you. At the front of this document there is place for you to write down this information.

Get a Cable Lock and Use It

Over 80% of the laptops on the market today are equipped with a Universal Security Slot (USS) that allows them to be attached to a cable lock or laptop alarm. Although this will not deter thieves with bolt cutters, it will deter casual thieves! Cable locks are one of the cheapest and most cost effective solutions to deterring thieves. Locks generally cost between $20 and $40.00. Get into the habit of locking your laptop up whether you're working on it or storing it.

Before purchasing a security cable, there are a few things that you will need to know:

- Does your laptop have a Universal Security Slot (USS)? It is a small hole usually found on the upper right side of the laptop.
- Make sure the lock is sturdy. Tubular cylinder locks are preferred to tumbler locks.

A few companies that carry cable locks:

http://www.pcguardian.com
http://us.kensington.com/html/11179.html
http://www.laptopsecuritysolutions.com/index.html
http://www.flexguard.com/laptop_security_slot_locks.html

Laptop Doesn't Have a USS?

If your laptop does not have a USS, there are cable locks that use adhesive pads. While the adhesive pad is not as effective as attaching the cable to the laptop chassis, you shouldn't discount it! Many stores use these kinds of cable locks on their displayed equipment, such as laptops, PDAs, cameras, phones, etc!

Laptop Carrying Case

Keep your laptop in an inconspicuous case. Expensive looking, flashy cases will get more attention. And so do laptop cases that *look* like laptop cases - there is no doubt about what is being carried in them! You want to keep your carrying case as simple as possible. Many manufacturers have come out with laptop backpacks. They have all the padding and compartments that you find in traditional carrying cases, but they look so much more inconspicuous!

Some manufacturers of notebook backpacks:
http://www.targus.com/us/cases_notebook_backpacks.asp
http://www.radtech.us/Products/Backpacks.aspx
http://www.mobileedge.com/

NOTE: remember not to store data backups in your carrying case. Do not store confidential information on CDs, DVDs, or flash drives in your carrying case! These small items can be stolen very easily!

Label / Tag Laptop and All Accessories

More than 1700 computers are lost or stolen every day. According to the FBI, 97% of unmarked laptops are never recovered. Most thieves are not interested in the laptop itself, only the resale value of the laptop. A very easy way to make a laptop's resale value go down is to label it! Make sure that everything that can be labeled *is* labeled. The potential theft value of a laptop is greatly reduced when additional work is required to remove all identifying marks. Clearly marking your laptop in a conspicuous place will deter casual thieves and, if stolen, increase your chances for getting it back! You can do this several ways:

- Engrave the contact information on the laptop.
- Asset tags or labels are available from many sources (print shops, online, etc). The tags peel and stick like any sticker, but cannot be easily removed.
- STOP (stoptheft.com) offers a variety of products, including

permanent metal security plates. If the security plate is removed there is an identifiable "tattoo" that is chemically and indelibly etched into the laptop's case declaring the property is stolen (Stolen Property 1-800-488-STOP).

Asset Tags / Computer Label Companies:
http://www.stoptheft.com/site/index.php
http://www.camcod.com

LoJack for Laptops

There are companies that have created tracking software for laptops. Once the software is downloaded, your computer silently and securely contacts a monitoring center whenever it is connected to the Internet and every 15 minutes thereafter. It transmits data such as IP address, MAC address, gateway address, and telephone number if available. If the company is notified the laptop has been stolen, the company works with law enforcement agencies to obtain a legal search warrant compelling the source ISP to reveal the user's physical address should the laptop sign into the Internet. One company, Computrace, reports that it has recovered 3 out of 4 stolen laptops under their protection. The service is very affordable (approximately $50 for 1 year).

Computer Tracking Software:
http://www.lojackforlaptops.com/
http://www.thecyberangel.com/
http://www.absolute.com

In Sight / Out of Sight

As silly as it might seem to have to say this - always keep your laptop in your sight! This is especially important when at airports, hotels, conventions, etc. If you have to get up and talk to the gate attendant, take it with you. Don't turn your back on it! Qualcomm's CEO had his laptop stolen from the podium while he was doing a news conference and he was standing just several feet away from it! The hardware was estimated at about $4000.00, but the information carried in it was thought to be worth millions! (http://www.forbes.com/2000/09/19/mu5.html) Never assume that your laptop will be safe, even for a minute.

On the other hand, if your laptop is not going to be with you, keep it out of sight! You'd be surprised at how many laptops have been stolen because it was left on the front seat of a car! Put the laptop back in its bag; store it in a trunk or desk, cable lock it to something not easily moved, etc.

Laptop Alarms

A few companies have made alarms for laptops. There are 2 different kinds of alarms: motion detectors and separation zone type alarms. The motion alarms usually have various levels of sensitivity settings. A separation zone alarms (called an anti-lost alarm) is usually in 2 pieces. You create a zone and when one piece is moved outside the zone (that

you can set), an alarm sounds.

Alarm Companies:
http://www.roadnews.com/html/Reviews/TrackIt.htm
http://www.securitykit.com/soniclock30012.htm
http://www.gsmalarmsystem.com/ProductShow.asp?ID=488

Travel Tips

- **Backup:** Always backup any important data before taking your laptop anywhere.

- **Don't Need It?** Only take files that you will need with you. If you don't need confidential information on your laptop for your travels, don't take it!

- **Car-Safe:** If you take your laptop in the car on a regular basis, consider getting a car-safe for your laptop (http://www.car-safe.com). These portable safes can be stored in the trunk of a car as well as in hotel rooms, etc.

- **Car Rental:** Always rent a car with a locking trunk and never leave your laptop in a vehicle where a passing thief can see it. If possible, rent a car with an alarm system and no external stickers identifying it as a rental.

- **Carrying Case:** Use a non-descript carrying case when traveling. If a thief sees a bag that looks like a laptop case and has a manufacturer's logo on it, most likely there *is* a laptop in it!

- **Beware of payphones:** If you are at an airport or train station (or any public place) and need to use a payphone, be careful! Use the buddy system, or if you have to put the laptop down, place it in between your legs.

- **Staying at a Hotel:** While staying in a hotel, if you leave your laptop in a hotel room, anchor it securely to a metal post or fixed object.

- **Conventions and Conferences:** Thieves target business conferences because they know that people get comfortable around their peers. Thieves can walk in and out of conference rooms unnoticed! Keep your laptop with you. Lock it up when you can.

- **Make security a habit!** People are the weakest link in the security chain. Get into the habit of locking your laptop (whether you are working on it or storing it).

Now that we know how to protect our laptops from being stolen, we need to realize that even when you do everything right, it can still happen! Now we need to protect the data itself.

Data Security

What methods you choose to protect your data will, of course, depend on the data you have on your laptop. If all you do is check your e-mail and calendar, and you don't carry confidential information on your laptop, you can choose some of the basic protection methods. But if you *do* have confidential information, trade secrets, etc., you will want to take more stringent methods of securing your data.

Common Sense Rules

Use your common sense in regards to protecting your data. Here are just a few common sense reminders:

- Keep the amount of institutional data or confidential data stored on your laptop at a minimum. If you don't need to have it there - don't!
- Do not use options that "remember" your password. These options are strictly for convenience and should not be used, especially on a laptop.
- Don't write down your password and/or keep it with the laptop.
- Don't use passwords that someone could figure out easily, such as: spouse or children's names, birthdays, anniversaries, the word "password". (See the section on creating a strong password)
- Never leave your laptop unattended, even for a minute.
- Treat your backups, CDs and flash drives just as you do your laptop! Because these things are smaller (and can contain the same information as your hard drive), they can easily be lost or stolen.
- Use data encryption tools to protect confidential information that you must store on your laptop or PC.

Work With Academic Computing or District IS

There are several things that can be done to your laptop to make it difficult for an unauthorized user to gain access. You will need to work with the staff in your Academic Computing department or District IS on the below security measures:

Set a BIOS Password (Boot Password)

If set, the very first thing a thief will see when the laptop is turned on is "Please enter boot password" and they will know they are in for a load of trouble. If you don't know the password, the laptop will not boot up. Not that this is impossible to get around, but it is certainly a good deterrent! Set a complex password. Do not write it down or store it with the laptop!

Set a Login Password (Windows Password)
If you set a login password, you will be required to provide a login name and password for Windows to come up. Without it, Windows will not start. Again, just like above, not that this is impossible to get around - but it can't hurt! Anything that you can do to make it more difficult for an unauthorized user - all the better!

Disable the Guest Account
If someone doesn't know your password to get on your laptop, they can use a "guest account". Windows disables the guest account by default. But you will want to make sure that the account is not enabled on your laptop. For additional security, you can create a complex password for the guest account and restrict its logon 24x7 (24 hours a day / 7 days a week).

Rename the Administrator Account
Some will argue that this will not stop hackers because they can still go in and find it. But why make it easy for them? This can stop some amateur hackers.

Create a "Dummy" Administrator Account
Another strategy is to create a local account named "Administrator", then give the account no privileges and an impossible to guess complex password.

Prevent "Last Logged In User Id" to Display
When you press Ctrl+Alt+Del, a login dialog box appears which displays the name of the last user who logged in to the computer. This makes it easier to discover a user name that can later be used in a password guessing attack. This can be disabled using the security templates provided on the installation CD.

Disable the Infrared Port on Your Laptop
Not many people use their infrared port to transmit data. However, disabling it will prevent someone else from browsing your files from across the room without you knowing it! You can disable the IR port via the BIOS, or simply cover it with a small piece of black electrical tape.

Lock Down Unwanted Ports
You can password protect unwanted ports, such as the USB port (used for flash drives). By doing this, unauthorized users cannot transfer information using the USB port. When the laptop owner wants to use the USB port, they have to "unlock" the port via the device locking software by providing a password.
http://www.pcguardian.com/products/8500_usb_port_lock.html

Passwords

Passwords... we all have them. Sometimes we feel we have too many of them! But a password is your first line of defense. So, although passwords can be viewed as a bit of a pain, they are an important part of data security! We all tend to take the easy way out with passwords, unfortunately that also makes them way too easy for someone to guess, such as: using the word "password" for a password, never changing a password once we have it, having systems / websites remember our password for us so we don't have to enter or remember it, etc.

We need to look at passwords a little differently. After all, we don't want to just open our door and let an intruder in without a little fight! At the same time, we need to also make passwords a "do-able" thing. Below we will talk about passwords, the do's and don'ts, having strong passwords and giving you some tips on how to create strong passwords that you can still remember easily!

How Are Passwords Cracked?

Creating a strong password requires you first to understanding how passwords are cracked. The primary way a password is cracked is through a brute force "dictionary" attack. These are programs that try to guess a password by running though a series of common phrases or words in various combinations (number in front, in back, in the middle, even spelled backwards). Not only do they check hundreds of root words, they also check them in combination with number and symbol substitutions ("!" for an "i", "3" for an "E"). As if dictionary attacks aren't bad enough, there are also keystroke sniffing programs. A sniffer watches your keystrokes and can determine passwords for all kinds of things you may do on your computer: logging into your e-mail; signing into your network; signing into Banner; checking your bank balance; etc. Don't let your password be a weak link!

Most Common Passwords

PCMagazine says that the passwords listed below are the most commonly used passwords. If your password is on the list, change it immediately!

1. password
2. 123456
3. qwerty
4. abc123
5. letmein
6. monkey
7. myspace 1
8. password 1
9. blink182
10. (your first name)

Password Don'ts

Most people choose passwords they can easily remember. People tend to pick passwords or part of passwords that are directly related to oneself. Below is a list of poor password choices.

Do not use:

- One's name and/or initials
- One's account name

- Names of immediate family members
- Names, breeds, or species of pets
- Birthdays, either your own or members of your family
- One's vehicle make, model, year
- Hobbies, interests and related words
- One's job title, employer's name, or any job related word
- Street numbers or names, city, county, state or zip for home, work, family or friends
- Social security number for you or anyone in your family
- License plate numbers
- Birthplace
- University or college name, college major
- High School name
- Student or employee ID numbers
- Serial numbers from consumer products

Password Tips

Now that we understand a little of how passwords are broken, and what *not* to use in a password, here are some common sense password tips as well as tips for creating a strong password.

- A password should contain a variety of letters, numbers, and symbols. If the password is case sensitive, a variety of upper and lower case letters are suggested.

- Do not use letter or number sequences (abc, asdf, 123, etc).

- A password should be at least 8 characters long. It should contain within the first four characters at least three of the following: a lower case letter, an upper case letter, a number, and a special character.

  For example: **4Whippet** fulfills the requirements above, however is not a good password. **pW4hIpT?e** is a better password and uses the same keyboard strokes with the exception of the "?". The problem with this password is, even though it is a more secure password, it is not easily remembered. The user will most likely write it down so they can remember!

- So, noting the above, one technique for developing a strong password is for the user to think of a sentence or statement that is easy to remember: *"Tom and I love to go to National Parks for vacation."* Then just take the first letters of each word, substitute numbers and special characters, add some upper and lower case letters, and you come up with: **t&ILtog2Np4V**. Now you have a more secure password that is easily remembered! To anyone else this will look like gibberish. But to the user, it means something.

- Now that you have a secure password, we need to tell you to change it! You need to change your password on a regular basis. Here at the District we have adopted the recommendations by the Payment Card Industry Data Security Standards (PCI DSS) for Banner passwords. Users have to change their Banner passwords every 90 days. So, let

Banner be the driving force. When it is time to change your Banner password, change your other passwords as well!

- Protect your password! Although it seems silly to say, don't share your password with anyone! Do not write it down and store it with the computer.

NOTE: Banner and ARGOS passwords are NOT case sensitive. You cannot use the "@" symbol in a Banner password.

Encryption

When it comes to confidential data, the best rule of thumb is if you don't *need* to have it saved on your laptop, don't! However, we also realize that some will need confidential data on their laptop. All of the security measures we have talked about so far are still important. But with confidential data, you want to take extra precautions. Data encryption is a procedure in which plain (readable) text is converted into coded (unreadable) text to prevent anyone but the intended recipient from reading the data.

There are many companies that provide encryption software, some are freeware and some you have to pay for. Encryption complexity is determined by the number of bits it uses to encrypt. The higher the bit encryption, the more complex and harder to break: 128-bit encryption is much better than 40-bit encryption. In order to see encrypted files, the user must have the password. You can encrypt files, folders and even the entire hard drive!

The benefits to having encrypted files are straight forward. The drawbacks are a little more complicated:

- Encryption requires that you have a private key. Many times the private key is stored on your hard drive. Hackers know this and if your laptop is stolen, the hacker will look for the private key. It is kind of like a gun and bullets - never store them in the same place! So, it is best to NOT store your private key on your laptop.

- If you forget your key and don't have a backup of it somewhere else, you are most likely out of luck!

- There have been issues in the past about encrypting folders or files using the Windows XP encryption on a shared drive (such as the I: or J: drives).

- When you copy encrypted files to a CD or flash drive, they will most likely NOT remain encrypted! This puts confidential data at a big risk because now they are not only readable, they are on an easily lost or stolen media! To backup the information, you may need to copy the entire folder (not the information within) to keep the encryption. Work with your Academic Computing area or District I.S. to ensure that your backups remain encrypted.

One possible solution to some of the drawbacks is having the private key on a separate drive and to require a strong password. This is similar to using an ATM to access your money. To access your money, not only do you need your ATM card, but you also need a password. With some encryption software, in order to access your encrypted files, you need to have the key (a flash drive with the key) and a strong password.

Encryption Software

At this point in time, the District does not have a recommended encryption package. We are currently looking into various possibilities. Until we select a District-wide solution, you will need to work with your campus Academic Computing department or District IS to determine what is the best solution for you.

Just like everything we have talked about thus far, you need to remember that encryption is not the magic answer to all our security concerns. However, though it may not be perfect, encryption is a needed step in protecting confidential data. And just a reminder, if you don't need confidential information on your laptop - don't put it there!

Virtual Private Network (VPN)

A Virtual Private Network (VPN) is a private communications network often used to communicate confidentially over a public network. It is also an encryption technology where in the data that is passed between two points forms a VPN "tunneling session" that is encrypted and cannot be sniffed.

Using Banner or Argos

If you are going to use Banner or Argos away from the office, it is required that you use VPN to do so. This requires that VPN be set up on your laptop and a strong password for VPN access is created. If this is something that you will need, please contact your campus Academic Computing department or District IS.

Reporting if Lost or Stolen

If your laptop is lost or stolen, you need to report it immediately to your campus Academic Computing department or District IS. You will need to provide various information including:

- Your name and contact information
- Make, model and serial number of the laptop
- What kind of information is on the laptop? Is there confidential information?
- If there was confidential information, what kind? Was it encrypted?
- Do you have a backup of the information? When did you last do a backup of the information?

Contact Information

Below you will find various contact information.

Anaheim Campus, District Offices

IT Technical Support Manager . . . . . Tom Wallace
Helpdesk 808-4849
E-mail . . . . . ishelpdesk@nocccd.edu

Cypress College

Director of Academic Computing . . . . . Frank Smith
Helpdesk 484-7157
E-mail . . . . . helpdesk@cypresscollege.edu

Fullerton College

Director of Academic Computing . . . . . Nilo Niccolai
Helpdesk 992-7711
E-mail . . . . . helpdesk@fullcoll.edu

School of Continuing Education (SCE)

Director of Academic Computing . . . . . Fred Rocha
Helpdesk at Anaheim 808-4703
Helpdesk at Cypress 484-8874
E-mail . . . . . helpdesk@sce.cc.ca.us

Dictionary

Backup	To copy files to a second medium (disk, CD, etc) as a precaution in case the first medium fails.
CENIC	Corporation for Education Network Initiatives in California
Encryption	Data encryption is a procedure in which plain (readable) text is converted into coded (unreadable) text to prevent anyone but the intended recipient from reading the data.
FERPA	Family Education and Rights Privacy Act. FERPA defines what information is "directory data," or data that is permitted to be given out without the consent of the student.
Flash Drive	Also known as a thumb drive, or USB flash drive. A flash drive is a small, portable disk storage unit that plugs into a computer's USB port. The amount of data they can store varies, 64MB to 2GB.
Peripheral	A computer device that is not part of the essential computer, yet can be connected to the computer, such as: printers, modems, scanners, flash drive, etc.
Security	In the computer industry, security usually refers to techniques for ensuring

	that data stored in a computer cannot be read or compromised by any individuals without authorization. This can involve using passwords and encryption. Security can also refer to measures to be taken to keep a device from being lost or stolen.
USB	Universal Serial Bus. A way to connect a computer to a peripheral device. A single USB port can be used to connect: mouse, modems, keyboards, printers, flash memory, etc.
VPN	Short for Virtual Private Network. A Virtual Private Network is a private communications network often used to communicate confidentially over a public network.

References

http://www.sfgate.com/cgi-bin/article.cgi?file=/c/a/2004/04/05/MNGGP60LNV1.DTL
http://newsroom.ucla.edu/page.asp?RelNum=7571
http://news.com.com/MasterCard+breach+hits+40+million+accounts/2100-1029_3-5751886.html
http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html
http://www.nocccd.edu/Policies/PDFs/5040.BP_062005.pdf
http://www.gartnergroup.com
http://www.sonoma.edu
http://en.wikipedia.org/wiki/laptop_theft
http://itso.iu.edu/Protecting_Your_Laptop_Computer
http://www.pcguardian.com
http://us.kensington.com/
http://www.laptopsecuritysolutions.com/index.html
http://www.flexguard.com/laptop_security_slot_locks.html
http://www.targus.com/us/cases_notebook_backpacks.asp
http://www.radtech.us/Products/Backpacks.aspx
http://www.mobileedge.com/
http://www.stoptheft.com/site/index.php
http://www.camcod.com
http://www.lojackforlaptops.com/
http://www.thecyberangel.com/
http://www.absolute.com
http://www.forbes.com/2000/09/19/mu5.html
http://www.roadnews.com/html/Reviews/TrackIt.htm
http://www.securitykit.com/soniclock30012.htm
http://www.gsmalarmsystem.com/ProductShow.asp?ID=488
http://www.car-safe.com
http://www.pcguardian.com/products/8500_usb_port_lock.html
http://www.pcmag.com/
http://www.eweek.com
http://www.caveo.com
http://www.trackitcorp.com/

http://www.securityfocus.com
http://tech.yahoo.com
http://www.flmicro.com/home/documents/ITTrendsQ2-editorial-lowres.pdf
http://www.webopedia.com

C:\MyFiles\Training\Laptop Training\laptop.training.wpd
Revision Date: 06-28-07