NOAO's Laptop Security Tips

1. Never carry your laptop in an obvious laptop bag or carrying case. These are immediate flags for would be thieves. Small padded cases that fit just the laptop are available at most luggage stores. This allows you to carry the laptop safely in a hard or soft side briefcase.
2. Never leave your laptop unattended, even for a moment. Many thieves work in groups; one will distract you while the other carefully removes your laptop in its case.
3. Purchase insurance coverage for your laptop. If it is company property, be certain under what conditions a theft is covered. If the laptop is your property, check with your insurance agent and determine if it is covered under your homeowners or renters insurance. Also what theft situations are covered, such as on business or pleasure travel. If coverage is not provided, obtain additional coverage as rider to your policy.
4. Utilize a laptop security cable. We get numerous reports of laptop theft when the owner leaves his or her office or cubicle for just a moment to go down the hall or to get a drink of water. Another time to be cautious is during meetings, laptops are used, a quick break is called and when everyone returns, some of the laptops are missing. Remember thieves have better access than you might think and are very quick. Use the cable in places like hotel rooms, conference rooms, airport waiting areas, and libraries.
5. Lock the laptop in a filing cabinet or other secure, out-of-sight location when you leave the office.
6. Be especially cautious in airports. Don't put your laptop down or let it out of your sight through security checkpoints.
7. Be certain to back up all important data daily. Remember the hardest thing to replace when a laptop is stolen is the lost data. Imagine losing all your contacts, your calendar, your Word and Excel documents, years of digital photos -- whatever you value on your computer. And if you have confidential information or trade secrets on your laptop, then you have even greater security concerns.
8. Encrypt the most important data. The most valuable part of a stolen laptop is the data. Many groups have cash bounties out for particular information that can be resold for identity theft or competitive use.
9. Protect the data and access of the computer with strong password and or a hardware key device. Hardware key products include fingerprint identification devices or other access control devices that plug into the USB port.
10. Make sure that OS security patches and virus definition updates are kept up-to-date on a laptop even though connections to the NOAO network may be few and far between.

Here are nine ideas to help prevent data loss or theft:

1. The most basic advice is to regularly back up all of the important data on your laptop hard drive. DVD burners make this easy to fit on one disc, so get in the habit of doing it regularly. Use a thumb drive in between for backups.
2. Disable the Guest account in Windows. It's also a good idea to assign it a long string of random characters as a password, just for good measure.
3. Many hackers will try to log in to a Windows laptop using the Administrator account. Rename this account with something that does not look obvious. Some have even set up a dummy Administrator account as well.
4. Modify the OS on your laptop so that the last username used to log on is not displayed in the logon dialog box.
5. Don't set your laptop to automatically log into websites, and don't save passwords on your laptop to make login easier. Otherwise, a thief who has stolen your laptop can easily log into your accounts.
6. It's possible for someone to access your files even without touching your computer through the IR, Bluetooth or Wi-Fi ports. Disable unused ports (do you really use the IR port?) and keep as current as possible with security patches.

7. In addition, be careful about using Wi-Fi access. With unencrypted Wi-Fi, every password, email message, and Web page can be read by any other user on that Wi-Fi network. That means you should only use secure (encrypted) email and should never enter a password or confidential information on a webpage over Wi-Fi unless it is a secure connection. (If you don't know what that means, then don't use email and don't enter private information from your browser when using Wi-Fi.)
8. Use data encryption whenever possible. For users of Mac laptops, we recommend using encrypted disk images which can be created with the Mac OS disk copy utility. See **http://docs.info.apple.com/article.html?artnum=107333**. For users of Windows laptops, we recommend the free package TrueCrypt. See **http://www.truecrypt.org**.
9. Install a BIOS or firmware password on you laptop. Be sure to remember the password, though! Since a thief can remove the disk from your laptop and install the disk on another computer, A BIOS password is not a replacement for data encryption!

You can increase your chances of getting your stolen laptop back. Before your laptop is stolen, there are three simple things you can do to help increase the odds (at least a little) that you get it back.

1. Record your serial number in a separate location. You will need this to prove ownership of any recovered laptop. This is also important if you file an insurance claim.
2. Register your hardware with the manufacturer. You can contact them if your laptop is stolen, so if the thief ever sends it in for repair, you will be notified.
3. Put a tamper resistant metal asset tag on your computer. This will help police track down the legal owner.

Some Things to THINK about:

1. We can all learn to be more attentive to the people and our surroundings, so that we can protect our property and our lives.
2. Always be aware of your surroundings and the people in them.
3. Realize that you are the prospective PREY or VICTIM.
4. Always keep your belongings in your sight and preferably in direct contact with your body or a tether device.
5. Be suspicious of unusual activity and keep your property closer to you until this activity is over and any threat has diminished.
6. The use of laptop security cables to lock down your property or lock it together will significantly reduce the risk of theft.
7. Put a label or tape your business card to the top of your laptop. Too many business travelers are using the same brand and model of laptops leading to confusion and in some cases the picking up of someone else’s laptop when going through security. The business card or label provides identification quickly when retrieving your laptop or trying to prove ownership in a mix up or attempted theft.

A better understanding of how a successful theft of property is accomplished is the key to prevention. Always remember that you are the person in charge of your property and belongings. The extra attention to prevention can save an enormous amount of time trying to deal with and recover after the theft of property. You and the decisions that you make are the single most important resources in the prevention of theft.

1.0 Revision History

Initial Version	May 16, 2006
Updated:	November 19, 2006

Updated:	February 16, 2007
Updated:	February 22, 2007
Updated:	February 27, 2007
Updated:	March 2, 2007
Revised:	April 21, 2009