(http://www.uni.edu/its)

Protect your Laptop

Protecting your Home Computer

How much personal or highly confidential information is on your laptop? What would happen if somebody stole your laptop? Would they have more than just a machine, but the ability to steal your identity or discover your secrets? Laptop theft is extraordinarily common.

Protect your Laptop from Theft

First of all, you should protect your laptop from theft. Consider the use of various laptop locks when your computer might be at risk of theft--especially while in hotel rooms. Such locks are available in most office-supply/electronic stores and online. Kensington [1] is a popular manufacturer of such locks. You might also consider using a non-traditional laptop case to avoid advertising you have a laptop.

Other ides to consider:

- Make sure you have a password on all accounts on your laptop.
- On Windows machines, consider setting a system level password at startup. Consult your computer manufacturer's documentation for information on how to set a system password.
- Consider limiting what information is actually stored on your laptop. Store the data on removable flash drives or CDs/DVDs that are stored separately from your laptop.
- Remember to backup your data, so if your laptop is stolen, you still have access to your data.

Encryption

The preferred security solution for laptops is encryption [2]. Debate if you think your entire computer should be protected or just portions of it. Protecting your entire laptop uses full-disk encryption [3]. Using full-disk encryption guaranties that all temporary files and data on your machine is protected. Unfortunately, all the data will be available to any attacker who encounters the system turned on, as the decryption keys are always loaded into memory once you enter your password. File-based encryption comes in many forms.

Truecrypt [4] is a free product for available for most operating systems (Windows Vista/XP, Mac OS X, and Linux) that creates virtual encrypted drives that can be loaded as needed. It can also encrypt entire external drives. It uses the industry standard AES [5] algorithm, in addition to providing options for other strong algorithms [6]. Truecrypt can also provide full-disk encryption for Windows systems, see this page [7] for more information.

Windows Vista Enterprise and Ultimate can encrypt the entire drive of some systems using a feature called BitLocker [8]. Consult Microsoft?s documentation for instructions. BitLocker requires the use of strong passwords on the system.

Recent Macs have two built-in encryption options, one is FileVault [9] and the other is creating, mounting, and dismounting encrypted disk images using Disk Utility [10]. Consult Apple's documentation for information.

There are a plethora of other free and paid solutions for encrypting data. Be sure to use software that encrypts the data using

a strong algorithm, such as AES, and check that the software is made by a reputable vendor or has been adequately tested by security-minded individuals.

All of the above solutions require the use of a strong password to protect your data. Consult the section "Use Strong Passwords [11]" for ideas on creating passwords. Consider using passwords or passphrases that are over 16 characters long to truly protect your data.

If your Laptop is Stolen

If you laptop is stolen, make sure you report it to the proper authorities. These parties may include representatives from law enforcement agencies, as well as hotel or conference staff. If you have sensitive data on the system, you may need to monitor your credit report and/or close accounts. See the section "Learn What to do if Something goes Wrong. [12]"

Links:
[1] http://us.kensington.com/
[2] http://en.wikipedia.org/wiki/Encryption
[3] http://en.wikipedia.org/wiki/Full_Disk_Encryption
[4] http://www.truecrypt.org/
[5] http://en.wikipedia.org/wiki/Advanced_Encryption_Standard
[6] http://www.truecrypt.org/docs/encryption-algorithms.php
[7] http://www.truecrypt.org/docs/system-encryption.php
[8] http://technet.microsoft.com/en-us/windows/aa905065.aspx
[9] http://en.wikipedia.org/wiki/FileVault
[10] http://en.wikipedia.org/wiki/Disk_Utility
[11] http://www.uni.edu/its/support/article/719
[12] http://www.uni.edu/its/support/article/726