



University of Southern California
Department of Public Safety
Laptop Security

Basic Security Measures

Choose a secure operating system and lock it down

If you care about your data, pick an operating system that is secure. Windows 2000 Professional and Windows XP Professional both offer secure logon, file level security, and the ability to encrypt data. If you are running Windows 95/98/Me, anyone who picks up your laptop can access your data.

Enable a strong BIOS password

Foils would be data thieves right from the start by password protecting the BIOS. Some laptop manufacturers have stronger BIOS protection schemes than others, so do some homework before relying on this alone. Find out from your laptop manufacturer what the procedure is for resetting the BIOS password. If they absolutely demand that you send it back into the factory and don't give you a "workaround", you'll have a better chance of recovering the machine and maybe even catching the thief. (Both IBM and Dell scored well in our field tests) Also find out if the BIOS password locks the hard drive so it can't simply be removed and reinstalled into a similar machine.

Asset Tag or Engrave the laptop

Permanently marking (or engraving) the outer case of the laptop with your company name, address, and phone number may greatly increase your odds of getting it returned to you if you happen to carelessly leave it in a hotel room. There are also a number of [metal tamper resistant commercial asset tags](#) available that could help the police return your hardware if it is recovered. According to the FBI, 97% of unmarked computers are never recovered. Clearly marking your laptops deters casual thieves and may prevent it from simply being resold over the internet via an online auction.



Register the laptop with the manufacturer

We've become so used to throwing away the registration cards for all of the electronic items we buy every day, because we've learned that it just leads to more junk mail. Registering your laptop with the manufacturer will "flag" it if a thief ever sends it in for maintenance, and increases your odds of getting it back. It also pays to write down your laptop's serial number and store it 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.

Physical Security

Get a cable lock and use it

Over 80% of the laptops on the market are equipped with a Universal Security Slot (USS) that allows them to be attached to a cable lock or laptop alarm. While this may not stop determined hotel thieves with bolt cutters, it will effectively deter casual thieves who may take advantage of you while your sleeping in an airport lobby, leaving a table to go the bathroom, etc.. Most of these devices are between \$30 - \$50 and can be found at office supply stores or online. In addition to the quality of the cable, consider the quality of the lock. (Tubular locks are preferable to the common tumbler lock design) And remember: They only work if you use them properly. Tether them to a strong immovable and unbreakable object.





University of Southern California
Department of Public Safety
Laptop Security

Use a docking station

Unbelievably, almost 40% of laptop theft occur *in the office*. Poorly screened housekeeping staff, contractors, and disgruntled employees are the usual suspects. You can help prevent this by using a docking station that is permanently affixed to your desktop *and* has a feature which locks the laptop securely in place. If you are leaving it overnight, or for the weekend, lock your laptop in a secure filing cabinet in your office and lock your office door.

Lock up your PCMCIA cards

While locking your PC to desk with a cable lock may keep someone from walking away with your laptop, there is little you can do to keep someone from stealing the PCMCIA NIC card or modem that is sticking out of the side of your machine. When not in use, eject these cards from the laptop bay and lock them in a safe place. Your docking station should have a NIC card built into it at your desk, and if you are traveling you won't be connected to the network anyway. Even when they aren't being used, PCMCIA cards still consume battery power and contribute to the heat levels within your laptop while they are left inserted into their slots.

Use a personal firewall on your laptop

Corporate networks protect their Servers and Workstations by configuring a [firewall](#) to prevent intruders from hacking back into their systems via the company's internet connection. But once users leave the corporate buildings and connect to the web from home or a hotel room, their data is vulnerable to attack. [Personal firewalls](#) such as [BlackIce](#) and [ZoneAlarm](#) are an effective and inexpensive layer of security that take only a few minutes to install. Although Windows XP comes with a personal firewall, it does not attempt to manage or restrict outbound connections at all. We recommend using a good third-party personal firewall to secure your Windows XP workstations. If you want to test how much information your personal firewall "leaks out" to the web, try the online leak test at <http://grc.com/lt/leaktest.htm>

Consider other devices based on your needs

Since laptop theft has become such a big issue, the market has been flooded with a variety of security gadgets and gizmos. Motion detectors and alarms are popular items, as are hard drive locks. Biometric identification systems are also being installed on some laptop models which allows your fingerprint to be your logon ID instead of a password. Consider the cost and bulk of these items along with your risk of theft before you go all out on a security solution.

Use tracking software to have your laptop call home

There are a number of vendors that offer stealthy software solutions that enable your laptop to check in to a tracking center periodically using a traceable signal. In the event your laptop is lost or stolen, these agencies work with the police, phone company, and internet service providers to track and recover your laptop. [CompuTrace](#), [SecureIT](#), [Stealth Signal](#), and [ZTrace](#) provide tracking services for corporations and individuals.

Protecting your Sensitive Data

Use the NTFS file system

Assuming your using Windows NT/2000/XP on your laptop, use the NTFS file system to protect your data from laptop thieves who may try to access your data. FAT and FAT32 File systems don't support file level security and give hackers a big wide open door to your system.

Disable the Guest Account

Windows 2000 finally disables the guest account by default, but if you didn't build the image yourself, always double check to make sure the guest account is not enabled. For additional security assign a complex password to the account anyway, and restrict its logon 24x7.



University of Southern California
Department of Public Safety
Laptop Security

Rename the Administrator Account

Many hackers will argue that this won't stop them, because they will use the SID to find the name of the account and hack that. Our view is, why make it easy for them. Renaming the Administrator account will stop some amateur hackers cold, and will annoy the more determined ones. Remember that hackers won't know what the inherit or group permissions are for an account, so they'll try to hack any local account they find and then try to hack other accounts as they go to improve their access. If you rename the account, try not to use the word 'Admin' in its name. Pick something that won't sound like it has rights to anything.

Consider creating a dummy Administrator account

Another strategy is to create a local account named "Administrator", then giving that account no privileges and impossible to guess +10 digit complex password. This should keep the script kiddies busy for a while. If you create a dummy Administrative account, enabled auditing so you'll know when it is being tampered with.

Prevent the last logged-in user name from being displayed

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, and 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, or via Group Policy snap in. For more information, see [Microsoft KB Article Q310125](#)

Enable EFS (Encrypting File System)

Windows 2000 ships with a powerful encryption system that adds an extra layer of security for drives, folders, or files. This will help prevent a hacker from accessing your files by physically mounting the hard drive on another PC and taking ownership of files. Be sure to enable encryption on Folders, not just files. All files that are placed in that folder will be encrypted. For more information check out our [EFS Resource Center](#)

Disable the Infrared Port on you laptop

I don't know anybody who actual transmits data via the infrared port on their laptop, but we have been able to use the IR port to browse someone else's files from across a conference room table without them knowing it. Disable the IR port via the BIOS, or simply cover it up with a small piece of black electrical tape.

Backup your data before you leave

Many companies have learned the hard way that the data on your computer is more expensive to replace than the hardware. Always backup you laptop before you do any extended traveling that may put your data at risk. This doesn't have to take a lot of time, and you can use the built in backup utilities that come with Windows 2000. If your network doesn't have the disk space to backup all of your traveling laptop users, you may wish to look into some of personal backup solutions including external hard drives, CD-R's, and tape backup.

Consider using offline storage for transporting sensitive documents

Backing up your hard drive before you leave can help you retrieve your data when you return from your trip, but it doesn't do you any good when you're still out in the field. There are several vendors that offer inexpensive external storage solutions that can hold anywhere from 40Mb to 30GB of data on a disk small enough to fit easily into your pocket. By having a backup of the files you need with you, you can work from another PC in the event your laptop is damaged or missing. As a plus, many of these devices support password protection and data encryption, so your files will be safe even if you misplace the storage disk. [lomega](#) makes a variety of products that are ideal for road warriors. Their new [USB Zip Drive](#) is light enough for travel, doesn't require an external power supply, and each ZIP disk can hold up to 200 Mb of data. Our favorite new toy



University of Southern California
Department of Public Safety
Laptop Security

is the [Iomega PocketZip](#) drive that fit directly into your laptop's PCMCIA slot. The disks are only 2 inches wide and can hold 40Mb. Other solutions include [Imation's SuperDisk](#), and [Castlewood's Orb Drive](#). Remember, when traveling keep these disks on your person, not in your laptop case or checked baggage, and be careful when passing through the metal detectors at airport security checkpoints. For additional security, lock or encrypt the files and have them sent by FedEx or UPS to your destination hotel or office.

Preventing Laptop Theft

No place is safe

Never assume your laptop will be safe just sitting around. Treat as if it were \$1,000 in cash lying around, and lock it down using a cable lock or secure docking station. [Qualcomm's CEO](#) has his laptop stolen from him during a news conference while he was standing no more than 30 feet from it. A State department employee had his stolen from a conference room and lost his job. Despite a \$25,000 reward it was never returned. Never assume that your laptop is safe.

Use a non-descript carrying case

Nothing says "Steal me" like walking around a public place with a leather laptop case with the manufacturer's or your company's logo stamped to the side. Consider buying a form-fitting padded sleeve for your laptop, and carrying it in a backpack, courier bag, briefcase, or other common non-descript carrying case. For men, backpacks make it easier to keep your laptop with you when you go to the bathroom. (A prime target area for laptop thieves in hotels, bars, airports, and convention centers). If you are traveling in airports and train stations, consider putting small locks on the zippers of your case (especially backpacks) so no one can simply reach into your bag and rip you off as you are standing in line.

Beware of payphones...

Cell phones are great if you are within your calling area, but the lack of a nationwide standard means that business travelers often have to use the payphones in airports, restaurants and hotel lobbies. Incidentally, these are also places that thieves like to hang out. While you are worried about covering up your credit card number as you dial the keypad, opportunistic thieves are waiting to see if you set your laptop case down. If you are traveling with someone else, use the buddy system to watch each other's backs instead of making calls at the same time.

When traveling by air...

There are a number of sophisticated professional crime rings that prey on business travelers carrying laptops. They look for brand new, high-end laptops and often shadow the airport curb side check-in, airline and rental car check-in counters, airport shops and security checkpoints. Anywhere where you might set your laptop bag down for a minute to attend to other things, thieves may lay in wait. There is a well-known two-person scam that attempts to steal a business traveler's laptop as they pass through the security checkpoint. If the thieves can't steal your laptop while you are occupied with the security process, they will often wait until you have a seat in the waiting area or in the airport bar. *A good rule of thumb is that if there is a sudden diversion in front of you, a laptop thief is probably behind you.* A common scam is for a beautiful young lady to walk behind you, smear mustard on the back of your shirt (without you knowing it), and then stop you and gleefully offer to help you clean it up. While you are occupied with the shirt stain, her accomplice is standing a few feet behind you waiting for you to set down your laptop bag. Another 2-person scam involves one person dropping a semi-valuable item in front of you in the hopes that you'll chase them to return the item. While your back is turned, their accomplice calmly walks away with your laptop case.

When traveling by car...

While I was working for a large international oil company, 5 executives went on a business trip to Australia and rented an SUV. On their first day, they stopped at a restaurant to have lunch, put all



University of Southern California
Department of Public Safety
Laptop Security

5 brand new \$4,000 Dell laptops in the back of the Ford Explorer and went in to eat. An hour later they came out to find the back window smashed in and all 5 laptops were gone (along with their passports). This illustrates 2 points. Always rent a car with a locking trunk (not a hatchback/minivan/or SUV) and never leave your laptop in a vehicle where a passing thief can see it through the window. If you do place your laptop in the trunk, use your cable lock to secure it to the trunk lid so that they still can't take it easily even if they manage to open the trunk. If possible, rent a car with an alarm system and no external stickers identifying it as a rental. Thieves target popular lunch spots with crowded parking lots, and they often look for rental cars. If you store your laptop in the vehicle for any period of time, keep in mind that the extreme temperature ranges within the vehicle could wreck havoc with your laptop. In the summer, the inside of a parked car can reach temperatures that will melt your laptop's components. In the winter, LCD screens can freeze solid and split.

While staying in a hotel...

Savvy road warriors already know the hazards of leaving valuables in hotel rooms, and professional thieves know that business travelers almost always have a few goodies that can be sold for a quick profit. If you keep your laptop in your hotel room anchor it securely to a metal post or fixed object. Consider a motion alarm for your laptop as well as one for your room. When not in your room, consider locking your laptop up in the hotel's safe. (Make sure you get a receipt).

When attending conventions and conferences...

Laptop thieves target business conferences and conventions because they know you'll feel more comfortable around your peers. They look for events that use the same facilities for a few days, because they're counting on you to become lax as you become used to the surroundings and start to feel safe. Most conventions only check ID's at the beginning of the morning. By the afternoon when you're tired and have let your guard down, thieves can walk in and out of conference rooms without being challenged or even noticed.

Make security a habit

People are the weakest link in the security chain. If you care about your laptop and your data, a healthy dose of paranoia will help keep it safe. (We hope we haven't made you too paranoid!) Get into the habit of locking your laptop up when you're working with it, or when storing it. (A cable lock takes less time to install than it does for your PC to boot.) Use common sense when traveling and try to stay in physical contact with your laptop at all times. If you are traveling with trusted friends or business associates use the "buddy system" to watch each others back (and laptops). A determined thief or industrial spy may still be able to get your laptop if they set their mind to it, but why make it easy for them?