

Security of Laptops

Laptop computers are a prime target for theft from your office, your home, or at airports, hotels, railroad terminals and on trains while you are traveling. They are an extremely attractive target for all types of thieves, as they are small, can be carried away without attracting attention, and are easily sold for a good price. They are also a favorite target for intelligence collectors, as they concentrate so much valuable information in one accessible place.

Safeware, the largest insurer of personal computers in the United States, paid claims for the theft of 319,000 laptop computers during 1999. Of course, most laptops are not insured, so this is only a small fraction of the total number of laptop computers that were stolen during that year.

When a laptop is stolen, you don't know whether it was taken for the value of the information on the computer or for the value of the computer itself. This makes it difficult to assess the damage caused by the loss.

This topic offers guidelines for keeping your laptop from being stolen, discusses technical measures for protecting information on the laptop if it is stolen or entered surreptitiously, and notes special problems relating to traveling overseas with your laptop.

Protection of Laptops

The basic rule for protecting your laptop is to treat it like your wallet or purse. Your laptop is a more attractive target for thieves than your wallet or purse, and if you lose your laptop, the cost to you in money and inconvenience is probably greater than if you lose your wallet or purse. If your laptop has sensitive government, commercial, or scientific data on it, the loss may be valued in the millions.

Even in your office, unless it is a controlled secure area, it is advisable to keep your laptop out of sight when not in use, preferably in a locked drawer or cabinet. The Washington, DC police recently formed a task force to fight a surge in thefts from downtown offices; laptops were the thieves' preferred target.

Your laptop is especially vulnerable while you are traveling. Here is a summary of basic precautions during travel.

- Disguise your laptop. The distinctive size and shape of a laptop computer make it an easily spotted target for thieves. Carry it in a briefcase or other, preferably grungy-looking, case.
- Never let a laptop out of your sight in an airport or other public area. If you set it down while checking in at the airport counter or hotel registration desk, lean it against your leg so that you can feel its presence, or hold it between your feet.

- When going through the airport security check, don't place your laptop on the conveyor belt until you are sure no one in front of you is being delayed. If you are delayed while passing through the checkpoint, keep your eye on your laptop. See [Theft While Traveling](#) for discussion of techniques used to steal laptops at airports.
- When traveling by plane or rail, do not ever place the computer (or other valuables) in checked baggage. If your aircraft departure is delayed and you are directed or invited to deplane and wait in the terminal, take your computer and other valuables with you. Don't leave them unattended at your seat or in the overhead.
- Never store a computer in an airport or train station locker. If you must leave it in a car, lock it in the trunk out of sight.
- Avoid leaving your computer in a hotel room, but if you must do so, at least lower the risk of theft by keeping it out of sight. Lock it securely in another piece of luggage. Placing the computer in a hotel vault or room safe should make it secure from theft, but in some foreign countries it may not be secure from access by local intelligence or security personnel.
- Never keep passwords or access phone numbers on the machine or in the case. Do not program your computer's function keys with sign-on sequences, passwords, access phone numbers, or phone credit card numbers. If the machine is stolen or lost, these would be valuable prizes.
- Try to keep only software files on your laptop's hard drive. Store your data files on diskettes and carry them separately from the computer.
- Back up all files before traveling.
- Beware of power surges. Don't be connected to either power lines or a copper phone line during a storm with lightning.

While in any public place, such as an airplane or hotel lobby, don't have up on your laptop screen anything you don't want the public to know about. A survey of 600 American travelers found that over one-third admitted looking at someone else's laptop while flying. Younger travelers were the worst offenders, with 49 percent of the men and 40 percent of the women under 40 admitting they look at what their seatmate is working on. Most are checking to see *what* their fellow passenger is doing, while others are more interested in *who* they are working for.

Be prepared for the airport security check. You may be directed by airport security personnel to open and turn on your laptop to demonstrate that it is actually a functioning computer. Be sure the battery is charged or have the power cord handy. If you can't turn your laptop on, you may not be permitted to take it on board the aircraft. The airport security X-ray machines will usually not affect hard drives. Floppy diskettes, having less shielding, may be affected. If possible, pass these to the attendant for hand examination.

It is even more difficult to protect your laptop, and the information on it, when traveling in foreign countries where your laptop may be targeted as a treasure trove of information.

Precautions while traveling overseas are discussed in [Theft While Traveling](#) and [Security and Safety Recommendations](#).

Technology for Protecting Information on Your Laptop

Due to the very high risk and high cost of laptop theft, many products are being developed to protect the security of information in your laptop if it is stolen, prevent the surreptitious entry into files on your laptop, make it more difficult to steal a laptop, or make it easier to find a stolen laptop. Specific products are not discussed here, as the technology is changing so rapidly. The following general types of products are now available.

- Encryption software. Storing all data files in encrypted form will prevent disclosure of the data even if your computer is stolen.
- Software that hides information on your hard drive, so that it is not found by the average thief who steals your laptop or, for example, by an intelligence collector who gains surreptitious access to your laptop in your hotel room.
- Various types of locks, keys, and biometric identification devices designed to prevent anyone but you from using the computer, and perhaps to alert you to any unauthorized attempt to use your computer.
- Software utilities that wipe the hard disk clean when deleting sensitive data files. These overwrite the deleted data making it totally unrecoverable, as opposed to the normal Delete command that only deletes the "pointer" that allows the computer to find the file on your hard drive. The file itself is not deleted until it is overwritten by another file.
- Tracers that identify the location of a stolen laptop. When the stolen laptop is linked to the Internet, it transmits a signal to a monitoring station that identifies the user's telephone number or Internet account.
- Proximity alarms that go off if the laptop gets too far away from its owner or user.

Ask your system administrator or computer security specialist to evaluate which of the available alternatives best meet your needs.

Traveling Overseas with a Laptop

Your laptop is even more vulnerable to theft or unauthorized access while traveling abroad than in the United States. For discussion of this, see [Theft While Traveling](#) in the Risks During Foreign Travel module.

If you are traveling overseas, be aware that some countries have import restrictions on laptops. Check before you leave to avoid delays and possible confiscation. Also some countries do not allow encryption of telecommunications traffic within their borders -- because they want to be able to monitor your messages..

When you return to this country, U.S. Customs may try to impose an import tax if they think the computer was purchased abroad. There are several ways to establishing prior ownership. One is to carry with you a bill of sale for the computer and/or insurance policy endorsement showing the serial number. You may carry a property pass from your employer that shows the serial number. Or you may register your laptop and any other valuables that might be mistaken as imports with U.S. Customs prior to leaving the country. You can do this at the Customs Entrance and Clearance Desk at the airport in advance of your flight.