



# Security for portable and desktop computers

**M**ORE than 600,000 laptop thefts occur each year totaling an estimated \$720 million in losses.

The chances of a laptop being stolen this year are 1 in 10. Computer systems, especially laptops, are prime targets for theft because of their small size and portability. Almost all businesses depend on computers to some extent and the business interruption due to a stolen computer is at the very least inconvenient and can be significant. Even if a stolen computer is immediately replaced, it may be difficult to restore the data if adequate precautions have not been taken. As well, the data may contain personal or confidential information that could be used for fraudulent purposes.

To reduce the risk of theft, it is highly recommended that businesses implement and enforce a strict computer policy with specific attention given to laptops. It is common for computers to be stolen without signs of forced entry or during regular business hours. Computer security is simple common sense. Treating a laptop as if it were cash is a good way to think about it – you wouldn't leave a pile of cash on your car seat nor should you leave your laptop unattended. By following a few simple rules you can greatly improve your computer security.

## Laptop computers

- Keep a record of your laptop details, such as the make, model, and serial number of the computer.
- At the office or business, secure the laptop with a steel cable lock.
- Do not leave the computer on a desk or otherwise visible after hours.
- To carry the laptop, use an ordinary-looking bag, such as a briefcase.
- Never leave a laptop in the passenger compartment of an unattended vehicle. The trunk is better and the laptop can be secured with a cable lock to a permanent part of the vehicle for additional protection.
- Keep the laptop near you at all times. Do not leave it visible in your hotel or in an unattended meeting room.
- When traveling, never check a laptop as luggage. It may be stolen or seriously damaged by rough handling.
- At off-site meetings, make sure that all laptops are protected during breaks and the room is locked when unattended.

## Desktop computers

Desktop computers should be secured with one or several of the following devices:

- Steel cable locks – secured to hard to move objects, such as desks and cabinets.



- Disk drive locks/cover locks – an insert secured with a key that prevents unauthorized use of a disk drive.
- Enclosures – the computer is locked into the enclosure that is secured to a desk or cabinet.
- Lockdown plates – to secure a computer to a desktop.
- Alarm systems – motion alarms attached directly to a computer.

## Server computers

This new and very important class of computers is the result of the huge development of computer networks that are considered mission critical systems. Unfortunately, the physical security is usually neglected or improperly implemented. Serious attention should be given to the physical security requirements of the server room.

## Data backups

Data should be backed up on a regular basis on all your computers. A copy of the backup should be kept off the premises. This may be the only way to restore your data in the event your computer is stolen.

At Federated Insurance, we believe Loss Prevention is a critical component of your Risk Management Program.

The information provided is intended to be general in nature, and may not apply in your province. The advice of independent legal or other business advisors should be obtained in developing forms and procedures for your business. The recommendations are designed to reduce the risk of loss, but should not be construed as eliminating any risk or loss.

---

RICHARD FROST is loss prevention coordinator – National Associations, for Federated Insurance. For more information, contact the Federated Insurance Loss Prevention Department at 800/665-1934 or visit [www.federated.ca](http://www.federated.ca).