Laptop Theft, Know Before You Go

Why Criminals Steal Laptops

10 years ago when travelers were victimized the object of theft was cameras, five years ago it was camcorders, today it’s laptops. Criminals look at laptops as a good return on their “investment”. A good laptop can be worth up to $5,000. A criminal can sell a stolen laptop to an unsuspecting used computer store or pawnshop and easily receive up to half its value in cash. Not too bad when you compare that to the amount of cash a thief would get by targeting your wallet. How much money would they get from you, $60.00? It is easy to understand why your laptop is so desirable to a thief. In addition to the obvious monetary benefit, there is also a legal benefit to stealing property vs. someone’s money. Most career criminals know that the penalties for a crime against property (theft) are less severe than those of a crime against a person. So to sum it up, laptops are worth more than cash, and if you are caught stealing them the penalty is less severe.

What Criminals Do With Stolen Laptops

One of the easiest locations for a thief to get rid of a laptop is selling it on a street corner. If the thief is brazen enough, they will take it to a pawnshop or sell to a fence who in turn takes it to one of those computer swap meets held on weekends. In one of the cases the thief would walk into a pawn shop and tell the store employee that his sister died in an accident and the laptop was her’s, and he had no use for it. A good thief will then produce a phony drivers license or identification card and the pawn will never be traced back to him. Many people think because laptops have serial numbers they can be traced as stolen property. This is a false sense of security, less than ten percent of the victims had their serial numbers recorded for report purposes.

Used computer stores or repair centers

Question, if you bought your own laptop, where was it purchased or where would you purchase it? Chances are that it would be from some large computer store or retail outlet. Did you know these mega stores also sell used and refurbished equipment? Additionally, independent repair centers sell used equipment too. In essence, there is quite a large market for used, high ticket, fast evolving items such as computers, and many people who are trying to serve that need from retailers to thieves.

Computer swap meets

Swap meets are even less likely to be checked by law enforcement for stolen goods. People that sell computers at these events are unregulated and many, if not all, do not report their sales or purchases to the police department. The purpose for reporting your purchases is to verify that the property is not stolen. This is where those recorded serial numbers come in handy! If a thief does business with a swap meet vendor you can be sure it is virtually an untraceable transaction.

Here are a few other tips:

- Create an atmosphere where employees are regularly briefed about topics such as new scams involving laptop theft. This can be accomplished by conducting crime prevention seminars and using information mediums such as newsletters and interoffice E-mail systems.

- Establish a policy making the employee responsible for the loss of the laptop if they do not follow company policy for safeguarding it on the premises or if they lose it outside of the building. Communicate this policy in writing and get a signed statement of acknowledgment.

- Provide employees with adequate secure storage areas for their laptops, such as locked security closets, cabinets and lock down devices at desks and workstations.
- Create a procedure where the company's security department or managers can remove unattended laptops for "safekeeping" leaving a tag or sticker in its place. The sticker will let the employee know the laptop was removed for safekeeping and can be picked up at the security office or other designated area. This will immediately prevent the theft of the laptop and will make the employee more aware that the laptop could have been stolen. This procedure provides a means of tracking employees by placing a notice in their personnel folder.

- Keep an inventory of all company owned laptops and computers. Know to whom and where they are assigned. Maintain a record of serial numbers, including those on the hard drive.

- Employees that travel with laptops containing sensitive information should use removable hard drives and carry them separately from the laptop. Backup files should be made regularly.

- All laptops should be engraved or permanently marked so they can aid in recovery if found by police. Check with the manufacturer regarding appropriate marking locations and warranty criteria prior to marking.

- Promptly report thefts to your local police department
- Contact the manufacture of the laptop if it stolen. Many will make a computer entry so if someone were to call or send it in for service, the police and the owner would be notified.
- Protect your personal identification with a password ex. social security number or date of birth.

Employee responsibility

Each employee should be aware of the laptop’s value and why it is important to protect it from theft. The employee must take responsibility for the protection of the company’s information, and by taking this responsibility, they must take the time to learn how professional criminals operate. Some companies will allow employees to expense out an insurance rider on their personal insurance to cover laptop theft. The very least a traveler should do is always use a security device to secure the laptop in the office (41% of all laptop thefts are stolen from the office) and on the road.

Insurance and laptops

Insuring of laptops falls into three areas. The most likely scenario is that a laptop is the property of a company and thereby is self-insured. This means if it is stolen, the company pays for it out of its budget and the loss is not reported to an insurance company.

The second most common type of insurance would be an employee who has a laptop cover under his or her own personal insurance. The insuring of computers may or may not be covered under your homeowners insurance and it is highly encouraged that owners of laptops contact their primary insurance company. Most of the time computers are not coverage by homeowners or the coverage is minimal.

The third type of insurance would be Third party insurance. This insurance is issued by a company that primarily provides coverage for laptops and related items. This is probably the most extensive type of coverage on the market and covers a wide variety of situations, from damage to theft. For example if your laptop were damaged as a result of a power surge, this type of insurance would cover it. The premium for this type of insurance is based on the value of your laptop. It purchases by the value of the products when they were purchased. I would caution you to compare the type of coverage between different companies. You will be surprised with the variations and the particular incidents where particular companies may not pay the claim.

Credit Card Insurance and Laptops

Credit card insurance may be another avenue that might provide coverage. The coverage is very different between cards, and to be quite frank, a few cards provide a lot better coverage that others. Many of these cards, fall into the "Gold Card" category and insure products against theft and damage for the first 30 to 60 days. It is highly recommended that anytime you purchase an electronic item that your purchase it with one of these cards, it may not pay for the value of it if stolen, but it might pay for its repair if dropped.

Vulnerable Locations

Although the theft of a laptop computer can occur at any place or time, there are certain obvious locations—company offices, airports, hotels and conference centers, college campuses, libraries and hospitals — where incidents occur most frequently. So it obviously pays to pay particular attention to your machine at these locations. In places such as hospitals and libraries, laptops are stolen by people who either have or appear to have a legitimate reason for being there. This may include contractors, service persons, custodians, delivery persons or even vendors.
Additional tips to avoid laptop theft

Would you leave a bag filled with $3,000 in cash sitting in your car or alone in your hotel room? Of course not. Then why do you leave your computer sitting on the passenger seat or on your hotel desk while you are out. If you depend on a notebook computer for school or work, having it stolen would be a disaster. We won't bore you with mind-numbing stats about how many computers are stolen every year -- we'll just jump right into our tips.

Don't take your eyes off your laptop

Remember, most laptop thefts occur at hotels, airports, or while in the rental car. Criminals don't have to rob you with a gun for your laptop; they just have to wait for you to set it down when you make a call at the airport phone booth. If you do set it down, make sure it is directly in front of you - not to the left, right, or behind you. It just takes a second for a thief to make off with it.

Lock it down

If you were to leave your hotel room, would you leave a wallet sitting on the nightstand with $2,000 in it? Of course not. But you would leave a laptop. Never leave a laptop alone in a hotel room without locking it down with a cable lock. If you do not have one, make sure the laptop is secured with a laptop cable lock or audible security cable alarm hidden from view, or in the room safe (if it fits). Remember, good thieves are good actors and actresses. They simply walk into your hotel room when the maid is doing nighttime turndown service and says it is their room. They tip the maid and walk out with one of your bags. Also be very careful about leaving your laptop in hotel meeting rooms. Numerous laptop thefts that occurred when the owner just left the meeting room for a 5-minute break. A thief simply walks into a meeting room during break time in a suit and blends in. Pretends the laptop is his and walks out. No one is checking ID at the door of your meeting room.

Locking Cable Tips

- Do not leave laptops unattended, particularly overnight on desktops. If your desk is in a high traffic area or an area accessible by the public, secure your laptop anytime you're away from your desk.
- Do not position laptops near exterior windows where they are subject to a smash and grab type theft.

Storage in cars

- If a laptop must be left in a car keep it locked and out of sight, the trunk of your vehicle is best.
- While riding, place the case between the driver’s seat and the rear seat so it won't slide around.
- Avoid storage in very cold or very hot weather.

Disguise your laptop

- By carrying your laptop in a case designed for computers, you immediately alert thieves that you have a laptop, even before you take it out to begin working. Carrying your laptop in an ordinary piece of luggage or briefcase will help deter theft.

Management Controls

Tractability

- Engrave the company name/ID on all laptops.
- Maintain and keep current a list of assignees, assigned equipment serial numbers and software.
- Periodic review of laptops and serial numbers.

Training

Provide annual loss prevention training and periodic reminders to maintain adequate safety and security awareness. Written Policies and Procedures should cover items such as:
• Is the individual responsible and held accountable for the safety and security of the assigned equipment.
• Is the individual responsible in the event of loss of unsecured equipment.
• Require a signed copy of the policy statement from all computer assignees.
• Audit annually, policies, procedures and assigned equipment and software lists.
• Loss investigations must be done on all stolen equipment. Do not easily accept loss, damage or theft of company property. Investigate all accidents and publicize the results.

SOURCE

www.kevincoffey.com

The NCPD does not necessarily endorse the views expressed on these websites or guarantee the accuracy or completeness of information in them.

NCPD/SPIN