

- » Another type of alarm works by setting up a security perimeter for the laptop. Moving the laptop beyond the perimeter sets off an alarm, locks keys to encrypted files, and disables the computer, making it useless to unauthorized users.
- » Commercially available software can also provide a means of protecting your devices from intrusion and prevent thieves from getting to your personal data. Most mobile devices include the ability to remotely “wipe” or erase the data from the cell phone or tablet should your device be lost or stolen. Services provided by device manufacturers, such as “Find My iPhone” (available in the Apple App Store) or Google’s “Find My Phone” (available from Google Play) also enable you to track your device using a computer, but **YOU MUST REGISTER YOUR PRODUCT** and enable the app or service for it to work. Don’t wait until it’s too late!

### Report Thefts and ‘Brick’ Your Device

If a theft does occur, **REPORT IT IMMEDIATELY** to the police department. Users should have the make, model, and serial number available so police can file a complete report and enter the stolen electronic device information immediately on the FBI’s National Crime Information Center (NCIC).

If you have been the victim of a crime and your cellular-enabled phone or tablet was stolen, you can take measures to make it economically worthless to the individual(s) who have taken your property. The major cell carriers have agreed to “brick” devices for customers who report their device lost or stolen and request this service.

- ❶ If it is believed your phone is still active (turned on), detectives may request that you do not cancel your service immediately in order to assist with the investigation.
- ❷ If, after three days, the device is believed to be turned off, a detective will request that you contact your cell carrier and ask that your device be “bricked.”

### National Cell Carriers

|                      |                |                |                |
|----------------------|----------------|----------------|----------------|
| AT&T . . . . .       | 1-800-801-1101 | T-Mobile. . .  | 1-800-937-8997 |
| Sprint. . . . .      | 1-888-211-4727 | Verizon. . . . | 1-800-922-0204 |
| US Cellular. . . . . | 1-888-944-9400 | Metro PCS . .  | 1-888-863-8768 |
| Cellcom . . . . .    | 1-800-236-0055 | Nex-Tech . . . | 1-877-621-2600 |

### Get Involved!

No one individual or agency working alone can prevent crime. It takes police and citizens working in partnership. The District of Columbia’s community policing strategy provides many ways for police and communities to work together to prevent crime and build safer neighborhoods. These include regular Police Service Area meetings in your community, citizen patrols and more. To learn more about community policing activities in your neighborhood, call your local police district:

|              |  |               |
|--------------|--|---------------|
| 1st District | Main: . . . . . (202) 698-0555 . . . . .       | TTY: 727-8506 |
|              | Substation: . . . . . (202) 698-0068 . . . . . | TTY: 543-2352 |
| 2nd District | Main: . . . . . (202) 715-7300 . . . . .       | TTY: 364-3961 |
| 3rd District | Main: . . . . . (202) 673-6815 . . . . .       | TTY: 518-0008 |
|              | Substation: . . . . . (202) 576-8222 . . . . . | TTY: 576-9640 |
| 4th District | Main: . . . . . (202) 715-7400 . . . . .       | TTY: 722-1791 |
| 5th District | Main: . . . . . (202) 698-0150 . . . . .       | TTY: 727-5437 |
| 6th District | Main: . . . . . (202) 698-0880 . . . . .       | TTY: 398-5397 |
|              | Substation: . . . . . (202) 698-2088 . . . . . | TTY: 281-3945 |
| 7th District | Main: . . . . . (202) 698-1500 . . . . .       | TTY: 889-3574 |

### Know Something About a Crime? Don’t Keep It a Secret

If you have important information to share with the police, the Anonymous Crime Tip Line and Text Tip Line enables you to give MPD vital information anonymously. Just dial (202) 727-9099 or text to 50411 24 hours a day, seven days a week. Your name will not be used, only the information you provide. Your information could lead to a cash reward. For more details, see [www.mpdc.dc.gov/tipline](http://www.mpdc.dc.gov/tipline).



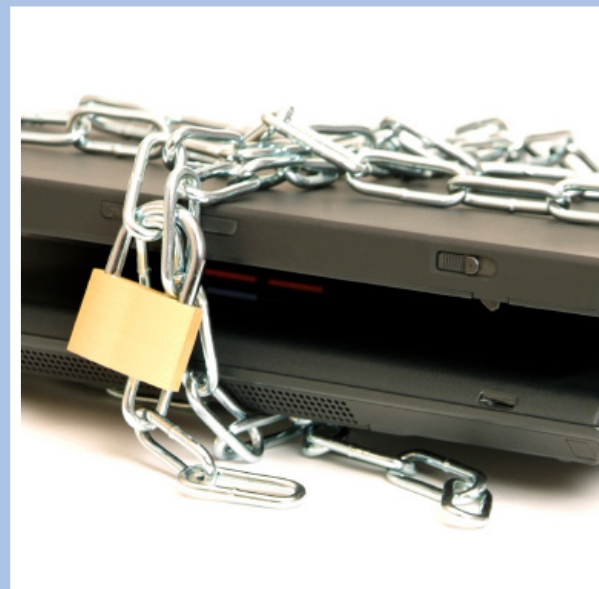
Have information for police?  
**CALL (202) 727-9099**  
**TEXT TO 50411**



GOVERNMENT OF THE DISTRICT OF COLUMBIA  
 Metropolitan Police Department  
 300 Indiana Avenue, NW  
 Washington, DC 20001

May 2013

**FOR YOUR SAFETY**



# Guarding Against Theft of Laptops and Personal Electronics

*Protecting Yourself and Your Property from Loss or Personal Injury*



# Your electronics can be replaced. You can't.

Laptop computer theft has been described as a 'high-growth' industry both in the United States and abroad. It is estimated that more than 300,000 laptop computers were stolen in the U.S. in 1999 alone.

## Why Do Crooks Steal Laptops and Other Electronics?

Laptop computers, tablets, cellular phones, and other personal electronics have become a target of choice for thieves all over the country. Why? Because they are small, valuable, can be removed quickly, are easily hidden, and there is a market for them. A thief can sell a stolen laptop, MP3 player, or other device to an unsuspecting used computer store or pawnshop, and easily receive up to half its value in cash.

Another reason criminals find these devices such an attractive item to steal is the legal benefit — most criminals know that the penalties for a property crime (theft) are less severe than those of a crime against a person (robbery).

## The Real Cost of Your Stolen Electronics

The cost of a stolen tablet, laptop, or other small electronic device is not just its replacement cost, but also the cost of peripherals and accessories, the installed software, the cost of configuring and loading replacement software, and the cost of lost time for the owner while the device is being replaced.

An even greater cost (especially if your employer issued your device) is the potential exposure and liability that results from lost confidential corporate and client information.

## How Can You Reduce the Risk of Having Your Electronic Devices Stolen?

Many times, often after the fact, we think about what we could have done to prevent valuables from being stolen. Here are a few tips to help you protect your personal electronics and laptop computer, whether you're at home, school, or on the road:

- » Don't leave your devices in an unlocked vehicle, even if the vehicle is in your driveway or garage, and **NEVER** leave it in plain sight, even if the vehicle is locked — that's just inviting trouble. If you must leave your devices in a vehicle, the best place is in the trunk. If you don't have a trunk, try to conceal them or fit them under a seat and lock the doors.
- » Carry your devices in a nondescript carrying case, briefcase, or bag when moving about. Placing these items in a case designed for computers is an immediate alert to

thieves that you have these valuable devices.

- » **DON'T** leave a meeting or conference room without your laptop or personal electronics. Take them with you.
- » Lock your device in a safe place when not in use or use a cable lock that wraps around a desk or chair leg.
- » Apply distinctive paint markings (such as indelible markers) to make your laptop unique and easily identifiable.
- » Consider purchasing a theft alarm system specially made for laptops and other electronics.
- » **BE AWARE** that if your computer is stolen, automatic log-ins can make it easy for a thief to send inappropriate messages with your account. Use password protection and require a person to log in every time the computer goes to sleep or powers down.
- » **BACK UP YOUR INFORMATION** using cloud-based storage or on portable media such as a CD, DVD, flash drive, or other backup media. Store the discs someplace safe.

## Flying with Your Laptop and Other Devices

- » Beware of this scam when approaching the X-ray scanner at the airport: The first person passes through the scanner quickly. The second person moves slowly, being delayed by pockets full of change, keys, etc. Meanwhile, the travelers stuck behind him have already placed their belongings — including laptops, cell phones, and tablets — on the conveyor belt. The first thief picks up the laptop as if it were his own and walks away while the other thief continues to hold up the line. **ONLY PUT THE LAPTOP ON THE CONVEYOR BELT WHEN YOU ARE NEXT IN LINE!** Keep your eye on your laptop, tablet, or other electronics as they come off the conveyor belt. And alert security personnel immediately if you think someone is attempting to steal your devices.

## Be Cautious When Leaving the Store with Your New Gadgets

Be cautious when making electronic purchases, particularly on days of new releases of popular devices and gadgets. Thieves know that these items will be more prevalent on release days as excited customers walk out of the store. If you have plans to make a major purchase of a popular computer, tablet, or phone, please remember these important safety tips:

- » If an **online tracking system** is available for your device, get the extra assistance in the store for setup before exiting the store.
- » **Don't be distracted** as you exit local cell phone stores and other electronic specialty stores that sell these items. Be deliberate as you exit these stores, concealing your purchase(s) and focusing on getting to your next destination. Cell phones and other music devices are major distractions when in use.
- » **Report suspicious people. Inside a store:** Do you notice people who are paying more attention to the purchases being made, rather than checking out new products? **Outside a store:** Do you see suspicious people standing at or near the exit for no real purpose? Report these behaviors to police.
- » **Try to shop with a friend.** Most victims who report crimes that involve snatching new products are people who have shopped alone. If you have an elderly parent, please make preparations to accompany him or her to make these kinds of purchases or suggest ordering them online.

## How Do Theft Prevention Technologies Work?

There are a variety of technologies that exist that can assist you in protecting your laptop computer and other electronics. Here are a few ways these systems work:

- » Two-way wireless security alarms for laptops consist of an alarm installed on the computer itself and a remote keychain device. If the alarm detects movement, it first checks whether you're nearby. If not, your keychain remote is alerted, emitting a "chirp." You can then choose to trigger the 110-decibel alarm on your laptop. The alarm can also be set to trigger solely on detecting motion.

