



Local Response | National Support

Preventing “Office Creepers” From Stealing Valuable Office Property

By J. Michael Coleman, Vice President of Commercial Real Estate, AlliedBarton Security Services

Today’s office environment features busy and mobile professionals who are continually on-the-go. We conduct conference calls on our cell phones, access the Internet with our PDAs and take thousands of files home by simply packing up our notebook computers. However, this convenience and portability has a price. Transportable electronic devices are easy prey for thieves who can resell the products on the street for a huge profit. Laptop thefts alone accounted for nearly \$6.7 billion in losses during 2004 – or an average of almost \$50,000 per company. Laptops sell on average for less than \$1,000 each on the black market, but the information on the hard drive is generally far more valuable than the hardware.

Many people who wouldn’t dream of leaving their computer or phone sitting in their unlocked car think nothing of leaving those items in an unattended cubicle at work. Technological advances have bred a new generation of criminals called “office creepers.” These individuals are dressed like your coworkers or building service personnel and rely on the anonymity of busy office buildings to shield them during their crime.



As Vice President of Commercial Real Estate for the largest American-owned security officer services company and a 30 year veteran of the physical security services sector, I have seen my share of office theft. I offer the following top ten tips to keep the “office creeper” at bay and to help protect your working environment:

Office Creeper 101 –An “office creeper” may skulk into your office dressed in uniform like a building engineer or in upscale casual ware or suit and tie to blend into the corporate culture. Try to become familiar with all of the co-workers in your immediate area. By knowing the identities of all your co-workers, you can easily identify an individual who may be out of place.

Flag and Tag the Wanderer – If you see someone unfamiliar wandering the halls or casually roaming about, ask if you can help them. Ask questions like “May I help you find someone?”

Honor Your Access Control Policy – If your building has an access control policy where visitors must wear a badge, you should notify security immediately if someone is walking around without proper identification. If you believe an individual seems suspicious, notify security. Be sure to note details about the person’s appearance so that you can provide a thorough description.

Sharing Isn’t Always Caring – Sharing can be great if you want to divvy up the contents of an office gift basket but *not* when your personal security is at risk. Never share keys or access

codes with anyone and never leave your office keys unattended. Keep your personal keys and office keys on separate rings.

Don't Hide Valuables in Plain Sight – While it may feel safer to tuck your wallet or purse into an unlocked cabinet drawer or under your desk, it's not as this is generally the very first place an office creeper looks. Position coat racks and hangers away from all doorways so that a thief cannot easily snatch items from the outside.

Lock & Mute – When leaving your office, make sure to lock the door and mute the telephone ringer. An unanswered phone is a clue to a thief that your office is empty.

Secure the Ties That Bind – Talk to management about purchasing a security cable for your laptop. This is an expensive locking device that secures your computer to the desk so that it cannot be easily removed.

Maintain Up-to-Date Inventory Log - Maintain an accurate inventory of all office equipment, furniture and devices in a locked, fireproof cabinet or other outside location (like your home office). And clearly mark all your personal electronics such as PDAs and cell-phones with identification. You can use non-removable tags or an inexpensive engraving pen.

Laptop Awareness – To avoid having your notebook be one of the 3,000 computers stolen each day, be sure to lock your notebook in your office during off-hours. Whenever possible, take your laptop home with you so you always know where it is. Keep only the most necessary proprietary information on your portable machine while updating your network with all sensitive information. Never load passwords onto your laptop and don't leave your computer unattended in a public place, even for a moment. Back up all your files and store that information some place other than your laptop carrying case.

Invest in Laptop Data Security Tools – Several effective laptop and data security options are available to protect your equipment from theft. IBM's new secure notebooks are equipped with *Asset ID*, a radio-frequency based security and asset-tracking technology. Automatic online backups by Toshiba prevent anyone from reading the data your computer sends without your pass phrase as information is encrypted before your PC transmits it. *Track-it* is a product that blasts a sonic alarm if you get more than 40 feet from your laptop to alert you that it has been left behind. CompuTrace is a software program that calls in with the location to a Central Monitoring System. These calls are made at regular intervals, providing the electronic serial number, phone number (from which it is calling) and other trackable information.

When traveling from your office, carry your notebook in a strong, padded non-descript bag. Don't use a carrying case that advertises there is a computer inside. Never leave your laptop in full view in your car and don't check your computer as luggage at the airport. Most office thefts can be prevented, and by following practical steps you can avoid becoming another police statistic.

###

For more information call 1-866-825-5433 or visit www.AlliedBarton.com.

About the Author: J. Michael Coleman is Vice President of Commercial Real Estate for AlliedBarton Security Services. Established in 1957, AlliedBarton Security Services is the largest American-owned security officer services company. He can be reached at: mike.coleman@alliedbarton.com