

HUB Canada



# DiMAGEine the possibilities

KONICA MINOLTA

HUB

DIGITAL
LIVING

Photo/Video Imaging  
 Brought to you by  
**KONICA MINOLTA**

Audio

Mobile

Personal Computers

Entertainment

Home Electronics

Classifieds
Shopping Guide
Contests
Media Kit

✉ e-mail this story
🖨 printer friendly version
📄 post a comment

## Lab Test: Stealth, smoke, and steel

By Dave Chappelle posted on 7/9/2003 9:40:21 AM

TCP Lab looks at theft prevention, recovery, and other security solutions

When you hear the term "computer security," you probably think of firewalls and anti-virus applications. They are important products-- something many of us have learned through experience (find more about these products in archived articles at [www.CanadaCompu](http://www.CanadaCompu))



Computer security also includes theft prevention and recovery for hardware and data. For this Lab, we've broadened our scope to include hardware and software products developed to prevent loss and assist with recovery of stolen hardware or data and to prevent unauthorized access and usage, data corruption, or inadvertent destruction.

## The software

### PC Phone Home/Mac Phone Home

From: Brigadoon Software, [www.pcphonehome.com](http://www.pcphonehome.com)  
 Estimated price: US\$29.95  
 Requires: Mac OS 8x, 9x, OS X; Windows 9x/Me/2000/XP; modem (dialup or broadband).

PC Phone Home helps get your stolen computer back. Once the software is installed, it sends an email message every time the computer is connected to the Internet. During setup, the system requires your email address and outgoing mail server name. No email client (email program or application) is needed. It's OK to use your own email address; just make sure that if you change ISPs, you also change the info listed with PC Phone Home. The ownership information you provide during registration must be accurate if

police are to be notified or legalities arise about providing false information on a warrant.

We used the same email address for sending and receiving, and each time we logged on, an email message appeared in the inbox within seconds. When connected on another telephone line using another ISP, it took about three minutes to receive the message. Dozens of information reports were sent stealthily, without any indication to the user that they were being issued.

The email messages from PC Phone Home contained all of the information we provided during registration, plus the IP address, time connected, user name, serial number, and even the silly name we forgot we'd given the computer when we first installed the operating system.

As PC Phone Home requires email to work, you might think formatting the hard drive or deleting the partition would wipe out the program. Wrong! It remains hidden as a separate, phantom partition disguised as a bad sector. Even if that is deleted, several key files spawn on reboot. Format and Fdisk commands don't work if the program is properly installed. Registered users can, however, request a special uninstall program to remove PC Phone Home. The company reports that all 31 computers registered with PC Phone Home that have been stolen so far in 2003 have been returned. None were tampered with, reformatted, or re-partitioned.

The user's manual describes a technique to slow down a thief: make your C:\ drive the first boot device in your system, and password-protect your BIOS settings. This prevents someone from using a floppy or CD to boot around the protection (many systems now ship with the CD-ROM drive set as the first boot option), and from readily changing the boot-drive order. It is possible to work around this protection, but it's more likely that many alerts will be sent before PC Phone Home is defeated.

We experienced one mildly annoying event. When not connected online, the dial-up networking adapter kept trying to dial a connection immediately after we booted up the computer. After leaving our computer running all night, we found dozens of dial-up attempts on our taskbar--so many that we couldn't close them, and were forced to reboot. By experimenting, we learned that simply closing the first two automatic dial-up attempts solved the problem. Note: if the program is configured for use with broadband, this should not occur.

A full version of the software can be downloaded from the PC Phone Home Web site, as can a free 30-day trial version for those who want to try before they buy. Enterprise versions are also available for organizations with several computers. PC Phone Home has no monitoring fees or other costs.


#### **SecurLock**

From: SecurSoftware, [www.secursoftware.com](http://www.secursoftware.com)

Estimated price: \$199 (1 key); \$278 (2 keys)

Warranty: 1 year

Requires: Windows 2000/XP; 1 MB disk space

 40-Lab-Securlock

A loss prevention device, SecurLock is a USB key/software solution for Windows 2000 and XP. (Note: key in photo indicates scale and is not part of SecurLock system) When inserted into a

\_\_\_\_\_ system, when inserted into a USB port on your system, it performs user logon authentication, file encryption, and storage for all of your passwords and logon profiles. It can store this type of information for several users on the same system.

If the "key" is removed from the USB port, you will be prompted to insert it when you boot the computer. If you insert it before turning on the system, or did not remove it when you last shut down the computer, you'll be prompted to type in the PIN you selected during setup. The computer can't be accessed at all without the SecurLock USB key. As well, SecurLock blocks access after three incorrect PIN attempts. At this point, only an administrator can unblock it. Of course, if you've installed SecurLock on a stand-alone system that only you use, you are the administrator.

Right-click on a file icon to encrypt it with either RC4 or Blowfish algorithm encryption. While it provides stronger encryption, Blowfish increases the size of files, so RC4 is recommended for larger files.

Right-clicking also offers the option of locking a file for transfer on floppy disk or by email, or making it self-extracting. Simply right-click, select the encryption or lock you want, and choose a password. To read the file, the recipient must also know the password.

The Single Sign-On (SSO) feature allows you to store all your logon names and passwords in one encrypted location. Each identity is stored under an icon with individual names. When you go to a Web site that requires a login, simply drag and drop the appropriate icon onto the Web page and click to enter rather than typing in a name and password.

Unlike some USB keys, SecurLock is internally shielded to protect it from static electricity damage.

#### **Kroll OnTrack Easy Recovery Lite**

From: Kroll OnTrack Inc., [www.ontrack.com/easyrecovery](http://www.ontrack.com/easyrecovery)

Prices: \$89 (Lite), \$199 (Data Recovery), \$499 (Pro), \$399 (File Repair)

Requires: 486 or faster CPU; 150 MB disk space

Kroll OnTrack Easy Recovery lets you try your hand at retrieving data lost due to corruption by viruses, accidental deletion, or drive failure. Easy Recovery probably won't cause a sudden decrease in business at professional data recovery labs--which OnTrack acknowledges by placing a Crisis Centre icon on your desktop during installation, with a direct link to its lab and other services.

For our tests, we downloaded a version of Easy Recovery Lite (the 26.6 MB file requires 2.5 hours to download at 33.6 Kbps). Through an easy-to-use Windows interface, the program offers data recovery and file repair, and is subdivided into recovery from various events. Depending on what caused your data loss, you can choose Formatted, Deleted, Virus, Standard, and Raw data recovery. Separate sections exist for repairing damaged Word and Zip files. Straightforward instructions are at the top of each window. You can also use Easy Recover Lite to make an emergency boot disk.

To recover a file, you must have two disks; a "bad" one with the damaged file, and a "good" one that Easy Recovery can write to. If not, you're gently reminded, "The destination path you have chosen is on the source partition. Please select a different destination."

We recovered both formatted and deleted files. Then we deleted and formatted again, and pressed the reset button on the system during a recovery, just to scramble things a bit. Using the Raw recovery function, which is reserved for the most extreme cases, our 400 KB Word file was fully restored, albeit with a different name. A small price to pay for what would have been lost otherwise. We'd love to say "we" recovered the data, but all we did was read and follow some instructions. Easy Recovery did the work.

A free trial version of the software can be downloaded from the Kroll OnTrack Web site.

### **eBlaster 3.0**

From: SpectorSoft Corp., [www.eblaster.com](http://www.eblaster.com)

Estimated price: US\$149.95, US\$99.95 (via Web)

For monitoring unauthorized computer use, eBlaster is personal spyware that generates detailed reports about the computer on which it's installed. Whenever that computer is used to access the Internet, a report is emailed to you, in intervals of your choice, from every 30 minutes to every 24 hours.

Select the online activities you want reported to you from the eBlaster Control Panel. Computer name, user login ID, IP address, keyword summary, applications used, Web sites and chat rooms visited, keystrokes typed, and the screensaver type are all included. If you set a Keyword Alert and that word comes up in an application, email, chat, or forum discussion, you'll know. In 30 minutes you can have individual keystrokes, nullifying your subject's password protection.

When specifying where you want the reports sent, keep in mind that spam filters on many email servers prevent you from seeing HTML mail. Choose the plain text report option for instant notification, and wait to view the full report later on the subject computer. At any time you may test the reporting function. Reports are sent to you with a bogus reply address, preventing a report from returning to the subject computer and possibly alerting the user.

There are no signs anywhere that eBlaster is installed on a computer. It doesn't appear in the program files or uninstall software. Few users are aware of the existence of the Windows Registry; but we looked thoroughly and found nothing. It has to be in there somewhere, but eBlaster hides very well.

Shouldn't your anti-virus program block an eBlaster installation? SpectorSoft says McAfee and Norton anti-virus programs won't stop even a remote installation of eBlaster, because the file is not a virus. Grisoft AVG was installed on our test system, yet eBlaster breezed right past it.

Our tests seem to indicate one or two known Windows exploits (security holes) are used to send the keyword alerts. Chat and messaging programs also have well-known exploits, which might also be used to send reports without a user's knowledge.

Two separate spyware detection applications couldn't detect eBlaster. Removing a known Microsoft Internet Explorer exploit disabled the eBlaster keyword reporting function, yet all other spying and reporting functions still worked.

The verification provided makes worried parents and employers obvious

users of eBlaster. However, SpectorSoft literature avoids mentioning that untrusting spouses form the largest portion of eBlaster purchasers.

## The hardware

### The Wrap

From: Security Solutions, [www.securitysolutions.ca](http://www.securitysolutions.ca), 416 410 9410; 888 410 9410

Price (incl. installation): \$275/\$325 (Wrap); \$425/\$475 (Server Wrap)

Note: Additional charge for installation outside Greater Toronto Area.

Dimensions (cm)	height	width	depth
The Wrap external	52	27.9	51.4-63.5
Max. PC size	48.3	24.8	46.4-57.2
Server Wrap external	55.2	35.6	90.2-101.6
Max. PC size	50.8	31.1	83.2-94.6



One look at this made-in-Canada 16-gauge steel "computer safe," which is attached to the floor, will send a thief looking for your cashbox or jewelry. Without a key, your computer will be destroyed before it ever comes out of this box.

Adjustable front and rear steel flat bars can be locked in position out of the way, or placed to prevent access to drive bays and card interfaces. The 1/2-inch rod pin locking mechanism with key cylinder lock is mounted on the front

bar. Keyed-alike locks are also available for locations with multiple units, such as a business, server room, or home with more than one computer.

The Wrap is shipped unassembled for compactness (four can be shipped in the space of one assembled unit).

While relatively easy to insert, the screws for assembling the Wrap are cross-threaded to discourage, if not prevent, removal once installed. The screw heads require an uncommon driver, which prevents anyone from taking it apart with a common slotted, Philips, or Robertson screwdriver.

Anchoring the Wrap is slightly more complicated than drilling into your concrete floor (over 90 percent of The Wrap installations are on concrete) with a masonry bit and Tapcons (typical hardware-store masonry screws). Unless you're experienced in concrete drilling and mounting, pay a little extra for installation. (Your insurance company may insist on a professional installer anyway.) If you have a wood floor, special mounting adapters are available that prevent a thief with a crowbar or lever from simply prying up

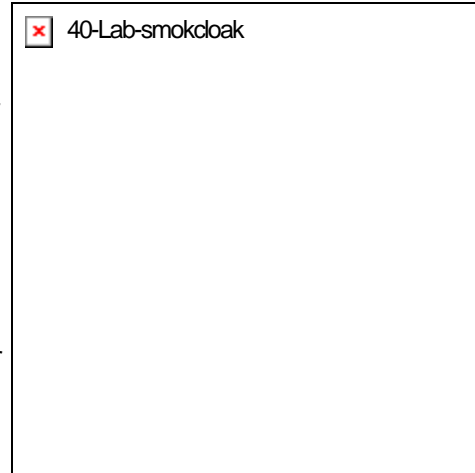
available that prevents most thefts from emptying out the entire package.

### Smoke Cloak

From: Martin Security Smoke, [www.smokecloak.com](http://www.smokecloak.com)  
Price: from \$3,000 (customized installation)

This loss prevention solution sports a "zero dollar loss" record, according to its manufacturer: nothing has ever been stolen from locations--which span the globe--where Smoke Cloak has been installed.

Smoke Cloak connects to existing security systems, so installations are customized for each location, with fire and police departments notified. It includes a separate battery so it works even in event of power failure at the location.



When the security system is breached, the Smoke Cloak quickly distributes smoke it has generated from distilled water and pharmaceutical and food-grade triethylene polyglycols, which won't harm those caught in the room with the smoke (though serious asthmatics might disagree). Unlike theatrical smoke, it leaves no residue. Smoke particles are one micron in size and non-buoyant. A "cloak sensor" measures the smoke level after the first "firing," producing more for half the duration if needed.

As a room fills rapidly with Smoke Cloak-generated smoke, thieves typically react by running from the "fire," according to the company. We witnessed a 140 sq. ft. room fill completely in under 15 seconds. With an additional 7.5-second blast, we couldn't see anything. With smoke from a fire, the air is clearer if you get close to the floor--not so here. Even on the floor, you can't see your hand until it touches your nose. It's an eerie feeling: an exit door and fresh air is only about a metre away, yet you're unsure of its direction.

Smoke Cloak backs up its reputation with money: public liability and damage loss insurance of up to \$20 million on unoccupied premises. The exception is first page output from copiers and printers, as the glycol on the drums could cause a bit of smearing on the first page. As well, normal smoke detectors are affected by this smoke, so have to be replaced (about \$30 each) in the event that the Smoke Cloak is used.

The level of the fluid used to make the smoke is monitored by the alarm monitoring station. The sensors shut down the pumps to save them in event of fluid depletion. Because the fluids evaporate at different rates, a licensed technician must service the system once a year.


Initially designed for banks and jewelry stores, this device now protects server rooms, labs, and other rooms used to house a lot of expensive equipment. Some home versions are installed near the main hall, activated by a panic button in the master bedroom.

Smoke Cloak renders ugly exterior window bars obsolete. Next time you pass an unbarred building in a shady area, you might be passing a Smoke Cloak location.

### Comments

There are currently 0 posted comments for this story.

---



[about us](#) · [permissions](#) · [editorial policy](#) · [view our TV ad](#)  
[HUB Pickup Locations!](#)