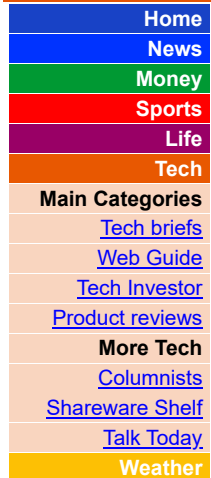


The Wayback Machine - <https://web.archive.org/web/20060504120338/http://www.usatoday.com:80/tech/columnist/200...>



Advertisement



CyberSpeak

Edward C. Baig

▪ [E-mail this story](#) ▪ [Subscribe to the newspaper](#) ▪ [Sign-up for e-mail news](#)

04/09/2002 - Updated 09:30 PM ET

Unlock the secrets of security for your laptop

Not long before the outbreak of the Persian Gulf War, a London crook lifted a laptop computer out of a parked car belonging to a British military officer. The computer eventually was recovered, but classified material supposedly was on the machine's hard drive, and the hapless officer was court-martialed and demoted.

Sadly, there is war again overseas, but then, as now, you need not harbor military secrets to fret about a potential laptop heist. Whether it's your personal finance data on Quicken or proprietary marketing plans that must be kept from an unscrupulous competitor, civilians routinely carry revealing bits best kept out of foreign hands. Of course, even when the stored information isn't so hush-hush, a bad guy (or gal) will gladly fence a notebook for a quick dollar.

According to the 2002 Computer Security Institute/FBI Computer Crime and Security Survey, the theft of laptops led to an average financial loss of \$89,000 among the corporations and government agencies who responded. (Only a small percentage of the sum actually relates to the hardware cost.)

Safeware, an insurance firm that will let you take out a policy on a laptop, reports that 591,000 notebooks were snared in 2001, a 53% rise over the previous year.

Lately, given the more stringent security measures implemented at airports since Sept. 11, the problem appears to be getting worse. Travelers are forced to remove laptops from their bags, and some passengers are inadvertently leaving the computers behind at checkpoints or absent-mindedly grabbing the wrong one. (Many models do look alike.) And crooks might be licking their chops over the high-tech booty coming through the X-ray scanner, provided the presence of armed soldiers doesn't discourage them.

You might lessen the likelihood of someone mistakenly walking off with your machine in the terminal by affixing permanent labels with your name and office number or by using colorful tape to make your notebook stand out.

Indeed, you can safeguard your portable with common sense.

Consider that, as dopey as it seems, some folks actually stick Post-it notes with corporate network passwords on the outside of the machine. That's like handing a bank robber the combination to the vault. I don't mean to be unsympathetic here, but YOU PEOPLE DESERVE TO GET RIPPED OFF.

Your car may stop you from falling asleep at the wheel

It's the middle of the night and you're alone, driving along a monotonous stretch of highway. The eyes are growing heavy. You are an accident waiting to happen.

Suddenly, a voice barks out: "Tell me the name of the first person you ever dated" or "Where is it that you work?" If you're slow to respond or give an incorrect answer, the car turns into a virtual alarm clock on wheels.

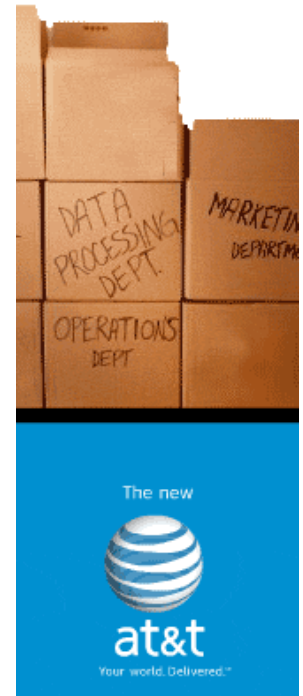
A window opens, the horn honks or the radio changes stations and raises the volume. You may be read aloud a pop trivia quiz or told a joke. Or even sprayed with water.

If all that doesn't rouse you, the system may book a motel room or direct you to the nearest rest stop.

Seem far-fetched? IBM researchers were recently granted a patent for an Artificial Passenger "telematics" system, a method of keeping fatigued drivers out of danger. Big Blue telematics guru Raj Desai says cars could be outfitted with a variation of the system within three years. (Telematics is a term that describes a gaggle of wireless safety, security, communications and entertainment services in a car, including remote diagnostics and e-mail.)

The ultimate cost of the system will be left to the manufacturer or provider. IBM's breakthrough is in detecting when the person at the wheel is about to enter la-la land.

Drowsy drivers are identified via a combination of speech and dialogue software. Slurred speech and changes in pitch are giveaways. Dashboard cameras may also pick up lip or eye movements.



Another tip: Kindly say no when the friendly fellow smiling at Junior volunteers to watch your laptop bag while you take the kid to the bathroom. Chances are he isn't an industrial spy, but why risk it?

In your hotel room or office, you may be able to thwart the casual thief with a simple lock or alarm, and there are many on the market. Among the accessories being sold at the Targus Web site, for example, is a new \$120 **DEFCON Authenticator**, a USB-based biometrics device that uses your fingerprint in lieu of a password to grant access to the operating system. No need for paranoia, but many computer crimes are inside jobs.

The technology is speaker-independent. But you'll also be able to personalize the system so Artificial Passenger will know the name of that first love and what it will take to wake you up, a spritz of H2O, perhaps.

A splash sure beats a crash.

— Edward C. Baig

I travel with an old standby called the Kensington **MicroSaver Security Cable**, which fits into a small slot on most notebooks. As with a bicycle cable, you wrap the \$45 steel cable around a desk or other immovable object to prevent an intruder from wandering off with the machine. Of course, if someone really wants the thing, they can snip the cord.

When the stored information is worth more to you than the physical hardware, you can load third-party programs to encrypt or scramble files so others can't read them. IBM recently started planting a security chip on the motherboards inside many new ThinkPad models. The chip, which adds about \$25 to the laptop cost, lets you encrypt files on the hard drive.

I recently put a new multipurpose laptop security package to the test, the \$99 **Anti-Theft PC Card** from Caveo Technology in Cambridge, Mass. The software and PC card combo product, for Windows machines only, aims to protect the computer and the information stored inside. It does so by sounding an alarm when someone grabs the machine and leaves your workspace. It also will prevent an unauthorized person from booting up. And you can encrypt confidential files.

The Caveo installation went fairly smoothly on a Windows 98 laptop, although I wasn't initially able to shut down the computer when asked to reboot. (I had to turn it off manually.) During setup, you choose a "theft perimeter," ranging from a distance of about five to 10 feet up to about 30 feet or more. An alarm goes off if someone takes the machine outside this predetermined zone.

You also can set up the system so that an alarm is activated whenever the screen saver comes on. Alternatively, you can create something called a "motion password," triggered when you physically position the machine in three distinct patterns. It's awkward. For example, you might activate the alarm by, in precise order, tilting the machine left, then right, then left again; the idea is that you can protect the machine with an alarm even when the computer is powered down.

If the alarm does go off, you must enter a 16-digit emergency PIN, different from the shorter PIN you use to boot up. All of this functioned properly, but after my testing was done, I had a hard time removing Caveo from my laptop, even with the help of a company techie. I suppose that speaks well for keeping the machine out of harm's way if a thief gets hold of it, but Caveo will need to address the issue for owners who want to legitimately uninstall the software.

So what happens if, despite your best intentions, your computer is pilfered anyway? Three services, **CompuTrace** from Absolute Software in Vancouver, British Columbia, **CyberAngel** from Computer Sentry Software in Nashville, and **zTrace** from zTraceTechnologies in Waltham, Mass., might just help you recapture the goods. Think of them as LoJacks for your laptop.

When an unsuspecting crook connects the laptop modem via a dialup or broadband hookup, software agents on the computer surreptitiously connect to a central monitoring center or the company's respective servers, blowing the cover on the IP address or phone number (via caller ID) used to call in. The modem speaker is kept silent. Working with law enforcement, these security companies can, we hope, locate your computer. The annual cost of monitoring for an individual ranges from \$50 to \$60. Coming soon: schemes for remotely retrieving, encrypting or wiping out files that get into the wrong hands.

I can offer one final tidbit to help you protect crucial content, if not the actual machine: Back up data as if your livelihood depends on it. As a British officer discovered a decade ago, apparently it does.

Send e-mail to Ed at ebaig@usatoday.com.



USATODAY.com partners: [USA Weekend](#) • [Sports Weekly](#) • [Education](#) • [Space.com](#)

[Home](#) • [Travel](#) • [News](#) • [Money](#) • [Sports](#) • [Life](#) • [Tech](#) • [Weather](#)

Resources: [Mobile news](#) • [Site map](#) • [FAQ](#) • [Contact us](#) • [E-mail news](#)
[Jobs with us](#) • [Internships](#) • [Terms of service](#) • [Privacy policy/Your California Privacy Right](#)
[Media kit](#) • [Press room](#) • [Electronic print edition](#) • [Reprints and Permissions](#)

[Add USATODAY.com RSS feeds](#) [XML](#)

© Copyright 2006 USA TODAY, a division of [Gannett Co. Inc.](#)