



Terrorism 2001 | Terrorism Shields Up

10/17/2001 By [Bill Goatse](#)

While Americans hang the Stars and Stripes from their windows, overwhelm the FBI with tips about suspicious-looking Middle Easterners, and tattoo the American flag on their forehead, Internet security experts say many are overlooking the most patriotic task of the time--securing their home computers from cyberjackers, foreign and domestic. "If people want to be patriotic, don't come to New York and dig through the rubble, go buy an anti-virus product today, right now," says Parry Aftab, executive director of CyberAngels, the world's largest nonprofit Internet security group. "Use it, update it, and keep the network up. [Cyberterrorists] could shut down our power, communications. If our network came down, we would be in trouble."

Aftab's sentiment echoes from her law office in New York all the way to Florida, where the state's terrorism task force has been working to secure government and commercial computer networks. "People might say, 'What does a hacker want with my computer?' But the point is that a hacker can use your computer as a weapon, like a bomb," says Tom Sadaka, special counsel to the Florida state prosecutor's office and a specialist in cyber crimes. "People have a moral obligation right now to not leave the keys in the ignition." Their warnings might seem alarmist, if not for the teenage hacker who created the Melissa virus two years ago and proved, indirectly, that vulnerable home computers could be a terrorist tool. The virus temporarily shut down the Web sites of CNN, Yahoo, eBay, and [Amazon.com](#) and caused \$80 million in damage. Then last year, with the help of personal computers, the "Love Bug" virus spread to computer systems at the Pentagon, NASA, and other federal agencies.

In the interconnected cyber world, home computers can participate in such attacks without the owner's knowledge or intent. "Preying on the lax security of the average home-computer user, attackers have found ways to plant malicious programs to give themselves remote control of home computers," Michael Vatis, director of Dartmouth College's Institute for Security Technology Studies, writes in a recent report on the threats of cyber terrorism.

So-called distributed-denial-of-service attacks, for instance, employ armies of "zombie" computers taken over by an outside computer to flood the victim's computer with e-mail and shut it down. Although the threats of viruses, worms, and hackers existed before the recent terrorist hijackings, historically, military conflict escalates cyber terrorism, not just by foreign enemies, Vatis says. Cyber terrorism by thrill-seeking hackers and sympathizers on both sides of the conflict cause a large portion of the costly static and destruction.

Vatis' study cites four cases where cyber terrorism increased following bloody attacks. Last year, for example, the kidnapping of three Israeli soldiers by Palestinians was

followed by pro-Israeli cyber attacks on the Palestine Authority. Pro-Palestinian hackers retaliated by taking down Web sites belonging to the Israeli Parliament, the Israeli Defense Forces, the Foreign Ministry, the Bank of Israel, the Tel Aviv Stock Exchange, and more.

Since the terrorist hijacking on Sept. 11, U.S.-based Web sites have been defaced with pro- and anti-American messages. Sadaka, who follows cyber crime cases for the state of Florida, says some authorities suspect a connection between the Sept. 11 attacks and the Nimba worm unleashed later that month, although it may have been created by an American youth.

That's not to say that the Osama bin Laden's Al Qaeda crew isn't computer savvy, or incapable of cyber terrorism. The CIA reported earlier this year that Al Qaeda member Ramzi Yousef, who was convicted of the World Trade Center bombing and an eerily familiar plot to blow up American jets in the Western Pacific, kept detailed plans of his diabolical deeds in an encrypted file on his laptop computer.

CyberAngels' Aftab notes that the Sept. 11 hijackers also showed cyber sophistication. "We know the Internet has been used by this group of terrorists," she says. "They were using it to coordinate the attack. We also have reason to believe they were using special encoding messages."

Federal law enforcement feared cyber attacks well before the recent terrorist strike. "One person with a computer and an Internet connection anywhere in the world could potentially break into critical systems, shut down an airport's air-traffic-control system, disrupt emergency services for an entire community, or launch a destructive denial-of-service attack," U.S. Attorney General John Ashcroft told a congressional committee on combating terrorism in May. "We are uniquely vulnerable. More than any other nation, the United States depends on computers and networks."

Cyber threats prompted the creation of the federal National Infrastructure Protection Center (NIPC) in 1998. However, the feds' success has been limited, according to a General Accounting Office report released in July. The agency criticized NIPC, which works out of FBI headquarters, for operating in a vacuum, by failing to communicate sufficiently with the private sector and other government agencies. All this at a time when a U.S. State Department report released in April predicted a growing cyber-terrorism threat.

Since Sept. 11, government and private efforts to protect the Internet--which was itself created by the U.S. military to assure communication in times of national threat--have intensified. NIPC is teaming up with private high-tech groups, sending out warnings of the most common vulnerabilities in computer systems. CyberAngels is distributing national public-service announcements pleading for computer hackers to team up and help stop cyber terrorism. State and local governments are working to update their computer security.

Experts warn that owners of home PCs should fortify their computers as well. Having anti-virus programs alone may not be enough protection. Such programs must constantly be upgraded, which in most cases can be accomplished with free downloads. "If you don't update it, you might as well not bother having it," Aftab says. "Make sure it's updated daily."

She also advises running any e-mail attachments through an anti-virus scan, even those

from someone you know. A lot of viruses will attach to listings in an e-mail address book. Computer users with cable and DSL service are even more vulnerable since their Internet connection remains constant. That's why Aftab and Sadaka advise downloading free firewall programs. "We can no longer be sloppy," Aftab says. "If we use good security programs, log off our computers when we leave the room, and start thinking about things the way the rest of the world does, we're going to be OK."

[Cnet.com](http://www.cnet.com) lists hundreds of are downloadable firewall and anti-virus programs, many free with customer ratings and reviews. CyberAngels and NIPC also offer tips on Internet security on their Web sites (<http://www.cyberangels.org/> and <http://www.nipc.gov/>, respectively).

And consider the other advantages: Firewalls can prevent criminals from stealing your credit-card and banking information online. And downloading a security program is a lot less painful and costly way to show your patriotism than getting a tattoo.

[Lynn Waddell is a freelance writer in St. Petersburg, Fla. This piece originally appeared in the Tampa alternative newspaper *Weekly Planet*.](#)