



Where Hackers Teach the Art of Self-Defense

*At a little school in Paris,
regular Joes learn how to
protect their cyberspace.*

By SUSAN CARPENTER, Times Staff
Writer

They call it the Hackademy. The so-called hackers school, on a dead-end street in a residential Paris neighborhood, is run by wiz kids who crack computer security codes as a sort of cyber-sport. Now they're taking what they've learned to the computer illiterati — regular people with a limited understanding of technology.

FOR THE RECORD

Hackademy computer school — A story in Southern California Living Jan. 29 about the Hackademy computer school gave an incorrect address for a related Web site. The site that lists computer security breaches is <http://packetstormsecurity.org>.

"We are trying to make the underground go overground," said a 23-year-old instructor who calls himself Fozzy, his English thick with French during a telephone interview. "Some hackers, not many, want to ... keep things [secret]. Us, we don't want to do like this. We want to give everyone the real picture."

While the school is small and in only one city so far, the Hackademy sees itself on the forefront of a coming consumer market — educating private individuals who want to defend their cyberspace.

Hackademy courses are taught in French, but they will soon be offered in English, due to interest from British and American computer users. The school's teachers are also considering offering English-language classes online.

As opposed to "black hats" (or "crackers" who break systems with malicious intent) and "white hats" (who discover system vulnerabilities and alert owners to fix the problem), the Hackademy's teachers call themselves "gray hats" — hackers who "do not do evil things" like write viruses or steal credit card numbers, but who break into computer systems "for our own entertainment" and to educate, said Fozzy.

Like the other handful of people who work at the Hackademy, Fozzy uses a pseudonym to conceal his identity, not from government authorities (with whom they say they've had no problem) but from other hackers. Fearing they will be targeted by "black hats" if they use their real names, the school's instructors use character names they've adopted from video games, books and movies.

According to the school's manager, who goes by the name Billy Dub, more than 400 people have attended the Paris Hackademy since it opened last fall. The school has only one classroom and six computers, but a second room is under construction and classes will be offered year-round.

Students, many of whom learned of the school

through media coverage and the Web, have included high schoolers, grandparents, businessmen, even a police officer. Most are 25 to 35 years old, though they range from 15 to 76. They are also mostly male, which prompted the school, upon opening, to offer free classes to the first 10 women who signed up.

About 90% of the students are "newbies," taking a beginners' course in basic vocabulary, introductory hacking techniques and how to secure their Web sites and e-mail. Classes about network vulnerabilities, exploiting network protocols and intruding systems are available to more advanced students, as are methods of protection from such attacks.

"Everybody should know what are the real security problems that exist on the Internet and how to protect from [them]. At this time, the [home computer] user really does not understand the problem," Fozzy said. "That is why we created the Hackademy."

What should they be worried about? Any number of things, Fozzy said, but most specifically the Web. As more and more services are performed online, and increasing amounts of highly sensitive personal data are shuttled through cyberspace, the Internet makes computers of all kinds more susceptible to attack.

The common misperceptions Fozzy hopes to correct: that antivirus software on its own prevents computers from acquiring bugs (it is useless unless security patches are applied)



and that credit card information is safe if sent over a "secure server" (it is not the transfer of data but how it is stored by the company on the other end that is unsafe, he said).

About 50% of the school's students say they have been the victim of some sort of security breach, according to Dub. Still, in a constantly shifting computer security landscape, one has to wonder: Is it even worthwhile for a layperson to bother educating himself on the latest techniques and strategies?

"No," according to Bruce Schneier, chief technical officer of Cupertino-based Counterpane Internet Security. "If you're worried about getting sick, you don't need to go to medical school. I go to a doctor so I don't have to become a doctor. If you're a layperson concerned about computer security, hire an expert."

There is no question computer security courses are imperative for large corporations. According to an annual security survey of Fortune 500 companies and large government agencies conducted by the Computer Security Institute in San Francisco, 91% of survey respondents in 2001 said they had suffered some kind of security breach.

To prevent computer break-ins, a number of American companies offer systems security classes, companies like Internet Security Systems in Atlanta and Foundstone in Irvine. Geared toward computer security professionals, their classes are usually taught by ex-military personnel and cost about \$1,000 per student per day.

By comparison, classes at the Hackademy target personal computer users and charge \$60 for nine hours of teaching by the hackers themselves. Then again, at least for now, you have to be in Paris.

Ultimately, it is the teachers who make the Hackademy unique — the collective of teen and 20-something self-taught computer hobbyists who, in the spirit of populist security, have gathered together to pool their knowledge and send it out to the world. With the exceptions of Defcon (a yearly hacker convention in Las Vegas) and monthly meetings around the country held by a group

called 2600, a formal group of hackers teaching hacking skills does not exist in the United States.

But it could, according to Mark Radcliffe, a Palo Alto-based Internet law attorney. The issue, Radcliffe said, is what is permissible by U.S. law. The Digital Millennium Copyright Act, passed in 1998, makes it illegal to crack somebody's system without permission or to distribute the tools that would accomplish those ends. Whether it is legal for hackers to teach what they know is largely a matter of intent.

"If they're saying, 'I'm going to crack Bank of America's security system,' that's not permitted. If they say, 'You have a computer at home with a DSL line and I'm going to crack into it and show you how your security is no good, and I have your permission to do that,' that's OK," Radcliffe said.

The basic concept behind courses offered by Foundstone and other corporate-oriented security classes and those offered by the Hackademy is basically the same. They both teach hacking skills as a means of defense.

"It takes a bad guy to catch a bad guy," said Jose Granado, national leader of Ernst & Young's Attack and Penetration Group. "The best way to stop an attack is to think like an attacker."

Ernst & Young, better known as an accounting firm, has been offering an antihacking class to corporate clients for six years. In a lab environment, instructors set up a dummy company with security situations common to many corporations. The students pretend they are hackers and play Capture the Flag, in which they infiltrate the system and, when successful, also scramble for the telephone to call their employers.

The name of the Ernst & Young class: Extreme Hacking. Other corporate hacking courses also capitalize on the buzz term, with courses titled "Ethical Hacking" and "Hacking and Cracking Seminar 101."

As for the Hackademy, the space in which it is located has all the trappings of subversion — artful graffiti on the walls, a pirate flag hanging

in a window — but the school's manager said both are more in the spirit of fun than sabotage. So is the Hackademy merely capitalizing on the hacker mystique for commercial gain, or do the school's instructors truly have an edge over those at other computer security schools?

"We try to be clever, to be at the edge of new things, to invent, to create new ways to go into the system," said Fozzy, who teaches a class on Web vulnerabilities, some of which he has found himself.

Granado agrees that hackers are on the cutting edge. But, he said, "Through our contacts in industry and through the conferences we attend and the mailing lists we're a part of, our folks have access to the same type of information that underground folks would have. We may get it a day later than some underground guy ... but over a very short period of time we'll have the same information as everyone else."

How? By monitoring news sources where hackers post their latest discoveries.

Not known for their modesty, many hackers delight in letting their peers in on the security breaches they've happened upon, on Web sites such as Rootshell.com and Packetstorm.com and in zines such as 2600: The Hacker Quarterly.

Perhaps the best-known American hacker magazine, 2600 (named for the hertz frequency that allowed phone hackers, or "phreakers," to place calls for free) details hacker tactics and highlights issues of concern to the community in its print edition. It also holds meetings for hackers to meet and exchange information.

The Hackademy is based on a similar concept. An offshoot of Hackerz Voice, a French-language newspaper for hackers founded by Publisher Olivier Spinelli in 2000, the Hackademy was initially founded to bring together its readers.

Spinelli, who has described himself as "an idealist trying to provide a public service," claims to have 80,000 subscribers in a handful of French-speaking countries, including Belgium, Switzerland and Canada.

The school has been much more popular than



its founders anticipated. There has been enough interest in Spain and Israel that Hackademies will soon be established in both countries, Dub said. There are no plans, however, to set up shop in America anytime soon.

"It's a good cause, but I think in the United States it will not be possible because of the lack of freedom after the new antiterrorism law," Fozzy said.

The school hasn't experienced any legal problems in France, according to Dub. But Radcliffe said a law similar to the Digital Millennium Copyright Act—the U.S. law designed to prevent copyright infringement in cyberspace—may be adopted by the European Union over the next few years.

Whether the dissemination of this information will result in good or ill remains to be seen. Just because the instructors are interested in helping people protect themselves doesn't mean that students will use what they've learned for such positive purposes. When you give someone the keys to a car, you can't control how they drive.

"I teach them ethical values," a teenage instructor who goes by the name Clad Strife (a character from the "Final Fantasy" videogame) told the BBC in December. "It's not my responsibility if they use my information to do something illegal at home."

