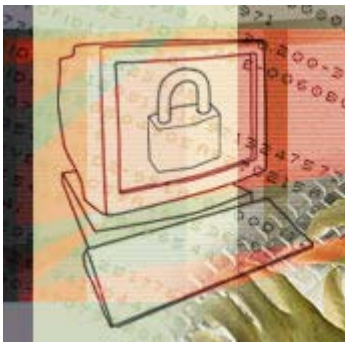
Kinko's spy case: Risks of renting PCs

Wednesday, July 23, 2003 Posted: 9:08 AM EDT (1308 GMT)



NEW YORK (AP) -- For more than a year, unbeknownst to people who used Internet terminals at Kinko's stores in New York, Juju Jiang was recording what they typed, paying particular attention to their passwords.
Jiang had secretly installed, in at least 14 Kinko's copy shops, software that logs individual keystrokes. He captured more than 450 user names and passwords, and used them to access and open bank accounts online. The case, which led to a guilty plea earlier this month after Jiang was caught, highlights the risks in using public Internet terminals at cybercafes, libraries, airports and other establishments. "Use common sense when using any public terminal," warned Neel Mehta, research engineer at Internet Security Systems.

Catching the culprit

Jiang was caught when, according to court records, he used one of the stolen passwords to access a computer with GoToMyPC software, which lets individuals access their own computers from elsewhere. The GoToMyPC subscriber was home at the time and suddenly saw the cursor on his computer move around and files open as if by themselves. He then saw an account being opened in his name at an online payment transfer service. Jiang, who is awaiting sentencing, admitted installing Invisible KeyLogger Stealth software at Kinko's as early as February 14, 2001. The software is one of several keystroke loggers available for businesses and parents to monitor their employees and children. The government even installed one to build a bookmaking case against the son of jailed mob boss Nicodemo "Little Nicky" Scarfo.

Boston College hit

Earlier this year, a former Boston College student pleaded guilty to using similar software on more than 100 computers around campus to collect passwords and other data so that he could create a campus ID card for making purchases and entering buildings illegally, authorities say. Mehta said that while millions of individuals use public terminals without trouble, they should be cautious. "When you sit down at an Internet cafe, ask the owner or operator about the security measures in place," he said. "If they don't know or don't have anything in place, you could consider going somewhere else." Encrypting e-mail and Web sessions does nothing to combat keystroke loggers. But encryption can guard against network sniffers -- software that can monitor e-mail, passwords and other traffic while it is in transit.

Cookies don't help

Data cookies also contribute to the risk of identity theft. Cookies are files that help Web sites remember who you are so that you do not have to keep logging on to a site. But unless you remember to log out, these files could let the next person using the terminal to surf the Web as you. Furthermore, browsers typically record recent Web sites visited so that users will not have to retype addresses. And such addresses often have user names and other sensitive information embedded. Secure public terminals should have provisions for automatically flushing cookies and Web addresses when a customer leaves, Internet security experts say. Kinko's spokeswoman Maggie Thill said the company takes security seriously and believes it has "succeeded in making a similar attack extremely difficult in the future." She would not provide details, saying that to do so could make systems less secure. Nonetheless, Thill said customers have a responsibility to "protect their information as they would a credit card slip." She said the company is trying to educate them through signs and other warnings. At one Kinko's that Jiang targeted, a sign attached to individual $18-per-hour stations warns: "BE SAFE. PROTECT YOUR PERSONAL INFORMATION."
