

# Growth of Wireless Internet Opens New Path for Thieves

*Source:* <http://www.derkeiler.com/Newsgroups/alt.computer.security/2005-03/0264.html>

---

*From:* MrPepper11 (*MrPepper11\_at\_go.com*)

*Date:* 03/19/05

Date: 18 Mar 2005 20:58:21 -0800

New York Times  
March 19, 2005

Growth of Wireless Internet Opens New Path for Thieves  
By SETH SCHIESEL

The spread of the wireless data technology known as Wi-Fi has reshaped the way millions of Americans go online, letting them tap into high-speed Internet connections effortlessly at home and in many public places.

But every convenience has its cost. Federal and state law enforcement officials say sophisticated criminals have begun to use the unsecured Wi-Fi networks of unsuspecting consumers and businesses to help cover their tracks in cyberspace.

In the wired world, it was often difficult for lawbreakers to make themselves untraceable on the Internet. In the wireless world, with scores of open Wi-Fi networks in some neighborhoods, it could hardly be easier.

Law enforcement officials warn that such connections are being commandeered for child pornography, fraud, death threats and identity and credit card theft.

"We have known for a long time that the criminal use of the Internet was progressing at a greater rate than law enforcement had the knowledge or ability to catch up," said Jan H. Gilhooly, who retired last month as special agent in charge of the Secret Service field office in Newark and now helps coordinate New Jersey operations for the Department of Homeland Security. "Now it's the same with the wireless technologies."

In 2003, the Secret Service office in Newark began an investigation that infiltrated the Web sites and computer networks of suspected professional data thieves. Since October, more than 30 people around

the world have been arrested in connection with the operation and accused of trafficking in hundreds of thousands of stolen credit card numbers online.

Of those suspects, half regularly used the open Wi-Fi connections of unsuspecting neighbors. Four suspects, in Canada, California and Florida, were logged in to neighbors' Wi-Fi networks at the moment law enforcement agents, having tracked them by other means, entered their homes and arrested them, Secret Service agents involved in the case said.

More than 10 million homes in the United States now have a Wi-Fi base station providing a wireless Internet connection, according to ABI, a technology research firm in Oyster Bay, N.Y. There were essentially none as recently as 2000, the firm said. Those base stations, or routers, allow several computers to share a high-speed Internet connection and let users maintain that connection as they move about with laptops or other mobile devices. The routers are also used to connect computers with printers and other devices.

Experts say most of those households never turn on any of the features, available in almost all Wi-Fi routers, that change the system's default settings, conceal the connection from others and encrypt the data sent over it. Failure to secure the network in those ways can allow anyone with a Wi-Fi-enabled computer within about 200 feet to tap into the base station's Internet connection, typically a digital subscriber line or a cable modem.

Wi-Fi connections are also popping up in retail locations across the country. But while national chains like Starbucks take steps to protect their networks, independent coffee shops that offer Wi-Fi often leave their connections wide open, law enforcement officials say.

In addition, many universities are now blanketing campuses with open Wi-Fi networks, and dozens of cities and towns are creating wireless grids. While some locations charge a fee or otherwise force users to register, others leave the network open. All that is needed to tap in is a Wi-Fi card, typically costing \$30 or less, for the user's PC or laptop. (Wi-Fi cards contain an identification code that is potentially traceable, but that information is not retained by most consumer routers, and the cards can in any case be readily removed and thrown away.)

When criminals operate online through a Wi-Fi network, law enforcement agents can track their activity to the numeric Internet Protocol address corresponding to that connection. But from there the trail may go cold, in the case of a public network, or lead to an innocent owner of a wireless home network.

"We had this whole network set up to identify these guys, but the one thing we had to take into consideration was Wi-Fi," Mr. Gilhooly said.

"If I get to an Internet address and I send a subpoena to the Internet provider and it gets me a name and physical address, how do I know that that person isn't actually bouncing in from next door?"

Mr. Gilhooly said the possibility of crashing into an innocent person's home forced his team to spend additional time conducting in-person surveillance before making arrests. He said the suspects tracked in his investigation would regularly advise one another on the best ways to gain access to unsecured Wi-Fi systems.

"We intercepted their private conversations, and they would talk and brag about, 'Oh yeah, I just got a new amplifier and a new antenna and I can reach a quarter of a mile,' " he said. "Hotels are wide open. Universities, wide open."

Sometimes, suspected criminals using Wi-Fi do not get out of their car. At 5 a.m. one day in November 2003, the Toronto police spotted a wrong-way driver "with a laptop on the passenger seat showing a child pornography movie that he had downloaded using the wireless connection in a nearby house," said Detective Sgt. Paul Gillespie, an officer in the police sex crimes unit.

The suspect was charged with child pornography violations in addition to theft of telecommunications services; the case is pending. "The No. 1 challenge is that people are committing all sorts of criminal activity over the Internet using wireless, and it could trace back to somebody else," Sergeant Gillespie said.

Holly L. Hubert, the supervisory special agent in charge of the Cyber Task Force at the F.B.I. field office in Buffalo, said the use of Wi-Fi was making it much more difficult to track down online criminals.

"This happens all the time, and it's definitely a challenge for us," she said. "We'll track something to a particular Internet Protocol address and it could be an unsuspecting business or home network that's been invaded. Oftentimes these are a dead end for us."

Ms. Hubert says one group of hackers she has been tracking has regularly frequented a local chain of Wi-Fi-equipped tea and coffee shops to help cover its tracks.

Many times the suspects can find a choice of unsecured wireless networks right from home. Special Agent Bob Breeden, supervisor of the computer crime division for the Florida Department of Law Enforcement, said a fraud investigation led in December to the arrest of a Tallahassee man who had used two Wi-Fi networks set up by residents in his apartment complex.

Over those Internet connections, the suspect used the electronic routing information for a local college's bank account to pay for online pornography and to order sex-related products, Mr. Breeden said.

The man was caught because he had the products delivered to his actual address, Mr. Breeden said. When officers went to arrest him, they found his computer set up to connect to a neighbor's wireless network. Mr. Breeden said the suspect, Abdul G. Wattlely, pleaded guilty to charges of theft and unauthorized use of a communications network and was sentenced to two years' probation.

In another recent case, the principal of a Tallahassee high school had received death threats by e-mail, Mr. Breeden said. When authorities traced the messages to a certain Internet Protocol address and went to the household it corresponded to, Mr. Breeden said, "Dad has his laptop sitting on a table and Mom has another laptop, and of course they have Wi-Fi, and they clearly didn't know anything about the threats."

Cybercrime has been known to flourish even without Wi-Fi's cloak of anonymity; no such link has been found, for example, in recent data thefts from ChoicePoint, Lexis/Nexis and other database companies.

But unsecured wireless networks are nonetheless being looked at by the authorities as a potential tool for furtive activities of many sorts, including terrorism. Two federal law enforcement officials said on condition of anonymity that while they were not aware of specific cases, they believed that sophisticated terrorists might also be starting to exploit unsecured Wi-Fi connections.

In the end, prevention is largely in the hands of the buyers and sellers of Wi-Fi equipment. Michael Coe, a spokesman for SBC, the nation's No. 1 provider of digital subscriber line connections, said the company had provided about one million Wi-Fi routers to its customers with encryption turned on by default. But experts say most consumers who spend the \$60 to \$80 for a Wi-Fi router are just happy to make it work at all, and never turn on encryption.

"To some degree, most consumers are intimidated by the technology," said Roberta Wiggins, a wireless analyst at the Yankee Group, a technology research firm in Boston. "There is a behavior that they don't want to further complicate their options."

That attitude makes life easier for tech-savvy criminals and tougher for those who pursue them. "The public needs to realize that all they're doing is making it harder on me to go find the bad guys," said Mr. Gilhooly, the former Secret Service agent. "How would you feel if you're sitting at home and meanwhile someone is using your Wi-Fi to hack a bank or hack a company and downloads a million credit card numbers, which happens all the time? I come to you and knock on your door, and all you can say is, 'Oops.' "