

# St. Petersburg Times ONLINE TAMPA BAY

[Weather](#) | [Sports](#) | [Forums](#) | [Comics](#) | [Classifieds](#) | [Calendar](#) | [Movies](#)

## Wi-Fi cloaks a new breed of intruder

**Though wireless mooching is preventable, it often goes undetected.**

By ALEX LEARY, Times Staff Writer  
Published July 4, 2005

---

ST. PETERSBURG - Richard Dinon saw the laptop's muted glow through the rear window of the SUV parked outside his home. He walked closer and noticed a man inside.

Then the man noticed Dinon and snapped his computer shut.

Maybe it's census work, the 28-year-old veterinarian told his girlfriend. An hour later, Dinon left to drive her home. The Chevy Blazer was still there, the man furtively hunched over his computer.

Dinon returned at 11 p.m. and the men repeated their strange dance.

Fifteen minutes later, Dinon called police.

Police say Benjamin Smith III, 41, used his Acer brand laptop to hack into Dinon's wireless Internet network. The April 20 arrest is considered the first of its kind in Tampa Bay and among only a few so far nationwide.

"It's so new statistics are not kept," said Special Agent Bob Breeden, head of the Florida Department of Law Enforcement's computer crime division.

But experts believe there are scores of incidents occurring undetected, sometimes to frightening effect. People have used the cloak of wireless to traffic in child pornography, steal credit card information and send death threats, according to authorities.

For as worrisome as it seems, wireless mooching is easily preventable by turning on encryption or requiring passwords. The problem, security experts say, is many people do not take the time or are unsure how to secure their wireless access from intruders. Dinon knew what to do. "But I never did it because my neighbors are older."

A drive through downtown St. Petersburg shows how porous networks can be. In less than five minutes, a *Times* reporter with a laptop found 14 wireless access points, six of which were wide open. "I'll guarantee there are tons of people out there who have their wireless network being exploited but have no idea," Breeden said. "And as we see more people utilizing wireless, we'll see more people being victimized."

### Prolific Wi-Fi growth

Wireless fidelity, or "Wi-Fi," has enjoyed prolific growth since catching on in 2000. More than 10-million U.S. homes are equipped with routers that transmit high-speed Internet to computers using radio signals. The signals can extend 200 feet or more, giving people like Dinon the ability to use the Web in the back yard of his Crescent Heights home but also reaching the house next door, or the street.

Today someone with a laptop and inexpensive wireless card can surf the Web via Wi-Fi at Starbucks or eat a bagel and send instant messages at Panera Bread. Libraries, hotels, airports and colleges campuses are dotted with Wi-Fi "hotspots." Even entire cities are unplugging.

"The information age is over. The information is out there," said Jim Guerin, technology director for the city of Dunedin, which will soon be the first city in Florida to go completely Wi-Fi. "Now it's the connectivity age. It opens up a whole new area for ethics, legal boundaries and responsibilities. It's a whole new frontier."

There's a dark side to the convenience, though.

The technology has made life easier for high-tech criminals because it provides near anonymity. Each online connection generates an Internet Protocol Address, a unique set of numbers that can be traced back to a house or business.

That's still the case with Wi-Fi but if a criminal taps into a network, his actions would lead to the owner of that network. By the time authorities show up to investigate, the hacker would be gone.

"Anything they do traces back to your house and chances are we're going to knock on your door," Breeden said.

Breeden recalled a case a few years ago in which e-mail containing death threats was sent to a school principal in Tallahassee. The e-mail was traced back to a home, and when investigators arrived, they found a dumbfounded family. The culprit: a neighborhood boy who had set up the family's Wi-Fi network and then tapped into it.

In another Florida case, a man in an apartment complex used a neighbor's Wi-Fi to access bank information and pay for pornography sites.

But he slipped up. The man had sex products sent to his address. "The morning we did a search warrant, we found an antenna hanging out his window so he could get a better signal from his neighbor's network," Breeden said.

Last year, a Michigan man was convicted of using an unsecured Wi-Fi network at a Lowe's home improvement store to steal credit card numbers. The 20-year-old and a friend stumbled across the network while cruising around in a car in search of wireless Internet connections - a practice known as "Wardriving."

(The name has roots in the movie *WarGames*, in which Matthew Broderick's character uses a computer to call hundreds of phone numbers in search of computer dialups, hence "war dialing.")

A more recent threat to emerge is the "evil twin" attack. A person with a wireless-equipped laptop can show up at, say, a coffee shop or airport and overpower the local Wi-Fi hotspot. The person then eavesdrops on unsuspecting computer users who connect to the bogus network.

At a technology conference in London this spring, hackers set up evil twins that infected other computers with viruses, some that gather information on the user, the *Wall Street Journal* reported.

Not all encryption is rock solid, either. One of the most common methods called WEP, or Wired Equivalent Privacy, is better than nothing but still can be cracked using a program available on the Web.

"Anybody with an Internet connection and an hour online can learn how to break that," said Guerin, the Dunedin network administrator. Two years ago when the city of Dunedin first considered Wi-Fi, Guerin squashed the idea because of WEP's inadequacy.

Dunedin's network, however, will be protected by the AES encryption standard, used by the Department of Defense. Passwords will be required, and each computer will have to be authenticated by the network. There also will be firewalls. "I'm confident to say our subscribers are at zero risk for that kind of fraud," Guerin said.

### Leaving the door open

Not everyone has sinister intentions. Many Wardrivers do it for sport, simply mapping the connections out there. Others see it as part public service, part business opportunity. When they find an unsecured network, they approach a homeowner and for a fee, offer to close the virtual door.

Some Wi-Fi users intentionally leave their networks open or give neighbors passwords to share an Internet connection. There is a line of thought that tapping into the network of a unsuspecting host is harmless provided the use is brief and does not sap the connection, such as downloading large music files. "There is probably some minority of people who hop on and are up to no good. But I don't know there is any sign it's significant," said Mike Godwin of Public Knowledge, a public interest group in Washington, D.C., focused on technology.

"We have to be careful," Godwin said. "There's a lot of stuff that just because it's new triggers social panic. Normally the best thing to do is sit back and relax and let things take their course ... before acting on regulation."

Randy Cohen, who writes "The Ethicist" column in the *New York Times Magazine*, was swayed by Godwin's thinking. When asked by a Berkeley, Calif., reader if it was okay to hop on a neighbor's Wi-Fi connection, Cohen wrote:

"The person who opened up access to you is unlikely even to know, let alone mind, that you've used it. If he does object, there's easy recourse: nearly all wireless setups offer password protection."

But, Cohen went on to ask, "Do you cheat the service provider?" Internet companies say yes.

"It's no different if I went out and bought a Microsoft program and started sharing it with everyone in my apartment. It's theft," said Kena Lewis, spokeswoman for Bright House Networks in Orlando. "Just because a crime may be undetectable doesn't make it right."

"I'll probably never know"

In a way Dinon was fortunate the man outside his home stuck around since it remains a challenge to catch people in the act. Smith, who police said admitted to using Dinon's Wi-Fi, has been charged with unauthorized access to a computer network, a third-degree felony. A pretrial hearing is set for July 11.

It remains unclear what Smith was using the Wi-Fi for, to surf, play online video games, send e-mail to his grandmother, or something more nefarious. Prosecutors declined to comment, and Smith could not be reached.

"I'm mainly worried about what the guy may have uploaded or downloaded, like kiddie porn," Dinon said. "But I'll probably never know."

--Times staff writer Matthew Waite contributed to this report. Alex Leary can be reached at 727 893-8472 or [leary@sptimes.com](mailto:leary@sptimes.com)

### **MINIMIZING THE RISKS**

Here are a few tips to minimize potential threats to a Wi-Fi network:

Enable WEP (Wired Equivalent Privacy). Even though WEP uses weak encryption and is breakable, it still provides an effective first measure of defense by encrypting the traffic between your wireless card and access point. Use 64-bit WEP to gain some security benefit without slowing down your network unnecessarily. You can also use WPA, a similar security protocol that's tougher to crack. Make sure both your access point and card support it.

Change your SSID (service set identifier) to something nondescriptive. You do not want to give out your name, address, or any other useful information to potential hackers. Also, don't use the default SSID.

Change the default password on your access points. The defaults of most network equipment are well known.

Enable MAC based filtering. Using this feature, only your unique wireless cards can communicate with your access point.

Turn off your access points when you are not using them. Why risk being scanned or being broken into if you are not using your wireless network?

Position your access points toward the center of your house or building. This will minimize the signal leak outside of its intended range. If you are using external antennas, selecting the right type of antenna can be helpful in minimizing signal leak.

Don't send sensitive files over Wi-Fi networks. Most Web sites that perform sensitive transactions like shopping with a credit card or checking bank account information use Secure Socket Layer (SSL) technology.

Sources: Force Field Wireless, [www.forcefieldwireless.com](http://www.forcefieldwireless.com) TampaBay.com columnist Jeremy Bowers.

© Copyright, [St. Petersburg Times](http://www.stpetertimes.com). All rights reserved.