You may think the only people capable of snooping on your Internet activity are government intelligence agents or possibly a talented teenage hacker holed up in his parents' basement. But some simple software lets just about anyone sitting next to you at your local coffee shop watch you browse the Web and even assume your identity online.

"Like it or not, we are now living in a cyberpunk novel," said Darren Kitchen, a systems administrator for an aerospace company in Richmond, Calif., and the host of Hak5, a video podcast about computer hacking and security. "When people find out how trivial and easy it is to see and even modify what you do online, they are shocked."

Until recently, only determined and knowledgeable hackers with fancy tools and lots of time on their hands could spy while you used your laptop or smartphone at Wi-Fi hot spots. A free program called Firesheep, released in October, has made it simple to see what other users of an unsecured Wi-Fi network are doing and then log on as them at the sites they visited.

Without issuing any warnings of the possible threat, Web site administrators have since been scrambling to provide added protections.

"I released Firesheep to show that a core and widespread issue in Web site security is being ignored," said Eric Butler, a freelance software developer in Seattle who created the program. "It points out the lack of end-to-end encryption."

While the password you initially enter on Web sites like Facebook, Twitter, Flickr, Amazon, eBay and The New York Times is encrypted, the Web browser's cookie, a bit of code that that identifies your computer, your settings on the site or other private information, is often not encrypted. Firesheep grabs that cookie, allowing nosy or malicious users to, in essence, be you on the site and have full access to your account.

More than a million people have downloaded the program in the last three months (including this reporter, who is not exactly a computer genius). And it is easy to use.

The only sites that are safe from snoopers are those that employ the cryptographic protocol Transport Layer Security or its predecessor, Secure Sockets Layer, throughout your session. PayPal and many banks do this, but a startling number of sites that people trust to safeguard their privacy do not. You know you are shielded from prying eyes if a little lock appears in the corner of your browser or the Web address starts with "https" rather than "http."

“The usual reason Web sites give for not encrypting all communication is that it will slow down the site and would be a huge engineering expense,” said Chris Palmer, technology director at the Electronic Frontier Foundation, an electronic rights advocacy group based in San Francisco. “Yes, there are operational hurdles, but they are solvable.”

Indeed, Gmail made end-to-end encryption its default mode in January 2010. Facebook began to offer the same protection as an opt-in security feature last month, though it is so far available only to a small percentage of users and has limitations. For example, it doesn’t work with many third-party applications.

“It’s worth noting that Facebook took this step, but it’s too early to congratulate them,” said Mr. Butler, who is frustrated that “https” is not the site’s default setting. “Most people aren’t going to know about it or won’t think it’s important or won’t want to use it when they find out that it disables major applications.”

Joe Sullivan, chief security officer at Facebook, said the company was engaged in a “deliberative rollout process,” to access and address any unforeseen difficulties. “We hope to have it available for all users in the next several weeks,” he said, adding that the company was also working to address problems with third-party applications and to make “https” the default setting.

Many Web sites offer some support for encryption via “https,” but they make it difficult to use. To address these problems, the Electronic Frontier Foundation in collaboration with the Tor Project, another group concerned with Internet privacy, released in June an add-on to the browser Firefox, called Https Everywhere. The extension, which can be downloaded at eff.org/https-everywhere, makes “https” the stubbornly unchangeable default on all sites that support it.

Since not all Web sites have “https” capability, Bill Pennington, chief strategy officer with the Web site risk management firm WhiteHat Security in Santa Clara, Calif., said: “I tell people that if you’re doing things with sensitive data, don’t do it at a Wi-Fi hot spot. Do it at home.”

But home wireless networks may not be all that safe either, because of free and widely available Wi-Fi cracking programs like Gerix WiFi Cracker, Aircrack-ng and Wifite. The programs work by faking legitimate user activity to collect a series of so-called weak keys or clues to the password. The process is wholly automated, said Mr. Kitchen at Hak5, allowing even techno-ignoramuses to recover a wireless router’s password in a matter of seconds.

“I’ve yet to find a WEP-protected network not susceptible to this kind of attack,” Mr. Kitchen said.

A WEP-encrypted password (for wired equivalent privacy) is not as strong as a WPA (or Wi-Fi protected access) password, so it’s best to use a WPA password instead. Even so, hackers can use the same free software programs to get on WPA password-protected networks as well. It just takes much longer (think weeks) and more computer expertise.

Using such programs along with high-powered Wi-Fi antennas that cost less than $90, hackers can pull in signals from home networks two to three miles away. There are also some computerized cracking devices with built-in antennas on the market, like WifiRobin ($156). But experts said they were not as fast or effective as the latest free cracking programs, because the devices worked only on WEP-protected networks.

To protect yourself, changing the Service Set Identifier or SSID of your wireless network from the default name of your router (like Linksys or Netgear) to something less predictable helps, as does choosing a lengthy and complicated alphanumeric password.

Setting up a virtual private network, or V.P.N., which encrypts all communications you transmit wirelessly whether on your home network or at a hot spot, is even more secure. The data looks like gibberish to a snooper as it travels from your computer to a secure server before it is blasted onto the Internet.

Popular V.P.N. providers include VyprVPN, HotSpotVPN and LogMeIn Hamachi. Some are free; others are as much as $18 a month, depending on how much data is encrypted. Free versions tend to encrypt only Web activity and not e-mail exchanges.

However, Mr. Palmer at the Electronic Frontier Foundation blames poorly designed Web sites, not vulnerable Wi-Fi connections, for security lapses. “Many popular sites were not designed for security from the beginning, and now we are suffering the consequences,” he said. “People need to demand ‘https’ so Web sites will do the painful integration work that needs to be done.”

This article has been revised to reflect the following correction:

Correction: February 25, 2011

An article in the Personal Tech pages on Feb. 17 about Wi-Fi users' vulnerability to hackers misspelled the name of a provider of virtual private networks, which can be used to thwart hackers. It is VyprVPN, not VyperVPN.

A version of this article appeared in print on February 17, 2011, on page B8 of the New York edition.

http://www.nytimes.com/2011/02/17/technology/personaltech/17basics.html?src=me&ref=general