Consumer Reports WebWatch
Cybercrime Prevention Project
Fact Sheet #10: Gone Wireless: Protect Yourself from ID Thieves and 'Freebooters'

This is the tenth fact sheet in Consumer Reports WebWatch's "Look Before You Click" campaign, supported by a grant from the New York State Attorney General's office, to help educate New York consumers about Internet fraud.

You might be using a laptop computer for home and business purposes. You may even have set up your own wireless network at home with routers, signal boosters and repeaters to reach all the rooms in your home. Did you know using Wi-Fi and home networks creates some unique security and privacy risks? Here's how to protect yourself from identity thieves, "freebooters" who steal your home wireless network signal, or hackers looking to attack your machine in the relative tranquility of a Wi-Fi hotspot at the airport coffee shop.

Remember that Wi-Fi hotspots are public places where people connect to the Internet. Using easily available software, others might be able to see what Web sites you are looking at, see your login information at sites not secured by SSL (chat rooms, for instance), and possibly see the contents of documents on your machine.

What to do? First, follow the same basic rules for computer security you've read about in our factsheets and on the Consumer Reports WebWatch site: Use an active anti-virus program (one that continuously installs updates based on the latest threats); install a spyware cleanser to remove badware from your machine; enable your firewall; and download security patch updates from your operating system's manufacturer.

Use encryption to scramble communications. If you have a choice, use Wi-Fi Protected Access (WPA), which is stronger than Wired Equivalent Privacy (WEP), though you may need to buy newer equipment. If you have access to a virtual private network (VPN), take advantage of its security, though if it's provided by your employer, you should consider what you will be using it for.

If the Wi-Fi service requires setting up payment for use, make sure you read all terms and conditions, and pay attention to security and privacy information. Finally, you may also want to consider doing your home banking and credit-card bill paying from a more secure, less public place.

The issues, and solutions, are similar when using a home network. Turn off identifier broadcasting on your wireless router, so it won't send a signal to any device in the vicinity announcing its presence. Turn off your wireless network when you know you won't use it. Make all your personal passwords tougher to crack, and reset manufacturer's default passwords. Also, don't write your passwords down on pieces of paper next to your computer or scribble them on the wall above your monitor. These are the first places a thief will look if your home is broken into.