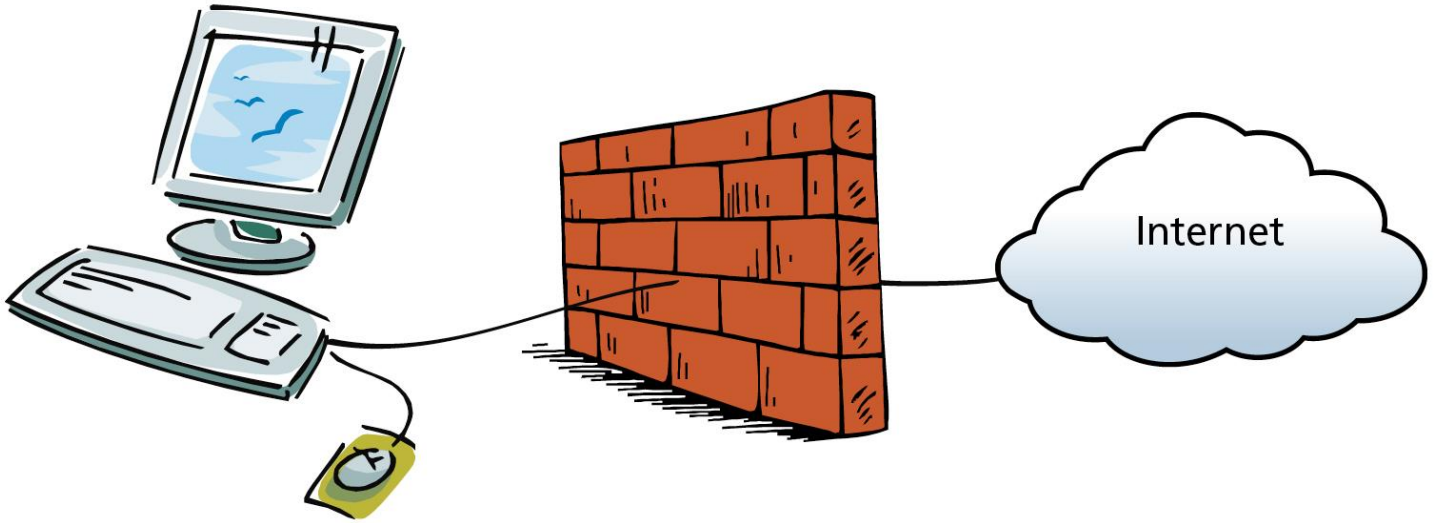
Firewalls

Firewalls are available for wireless routers as well as for client and server computers.

When browsing a wireless network, make sure your computer's firewall is enabled. If you're using your own router instead of one at a hotspot, configure the router's firewall too.

Remember, this will prevent unwanted network traffic from entering your network, because you can block network ports that you don't need.

FIREWALLS



Bluetooth Snarfing

Bluetooth devices, such as smartphones, often contain important information, such as an address book with phone numbers.

Since these devices can broadcast a signal via Bluetooth, hackers can access that signal and steal the phone's information, such as contacts' names and numbers. In one instance, hackers were able to do this with their own phone, as far as a mile away from the other phone.

The best way to protect information on your phone or PDA is to turn off the Bluetooth signal when you're not using it.

BLUETOOTH SNARFING

Keyloggers

One of the most dangerous risks on an unprotected wireless network, such as at a public coffee shop, is keylogger programs. Keyloggers are a type of software that logs your keystrokes and clicks.

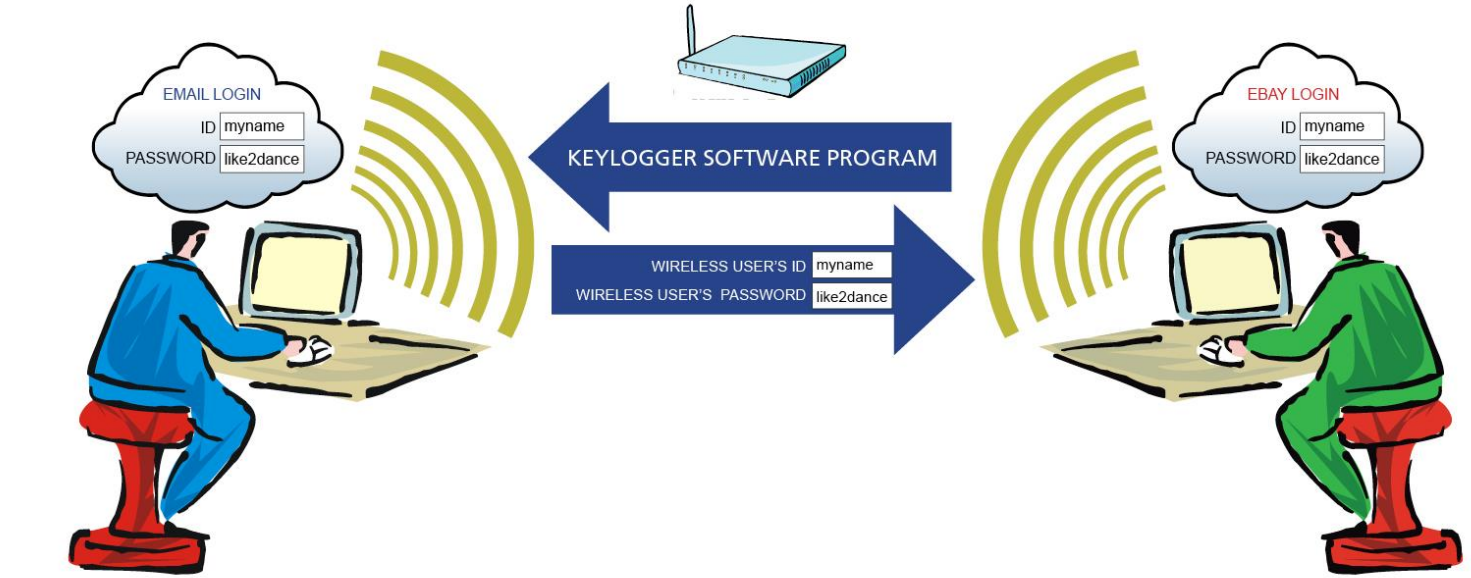
At a wireless hotspot, another person with a wireless connection can intercept your data stream, install a keylogger on your computer, and then have the software send your keystrokes back to his or her computer.

If you log in to bank accounts or your email, the keylogger will record your passwords, and the hacker will get access to your accounts and personal information. The hacker can use this information to charge your credit card, sell your information on the black market, or even lock you out of your accounts.

Note that keylogger programs can be installed on non-wireless connections as well. Software programs installed on computers or on devices that connect between the computer and the keyboard can do keylogging.

Protect yourself by using your firewall and preventing software from automatically installing itself on your computer.

KEYLOGGERS



WIRELESS USER

HACKER

Pharming

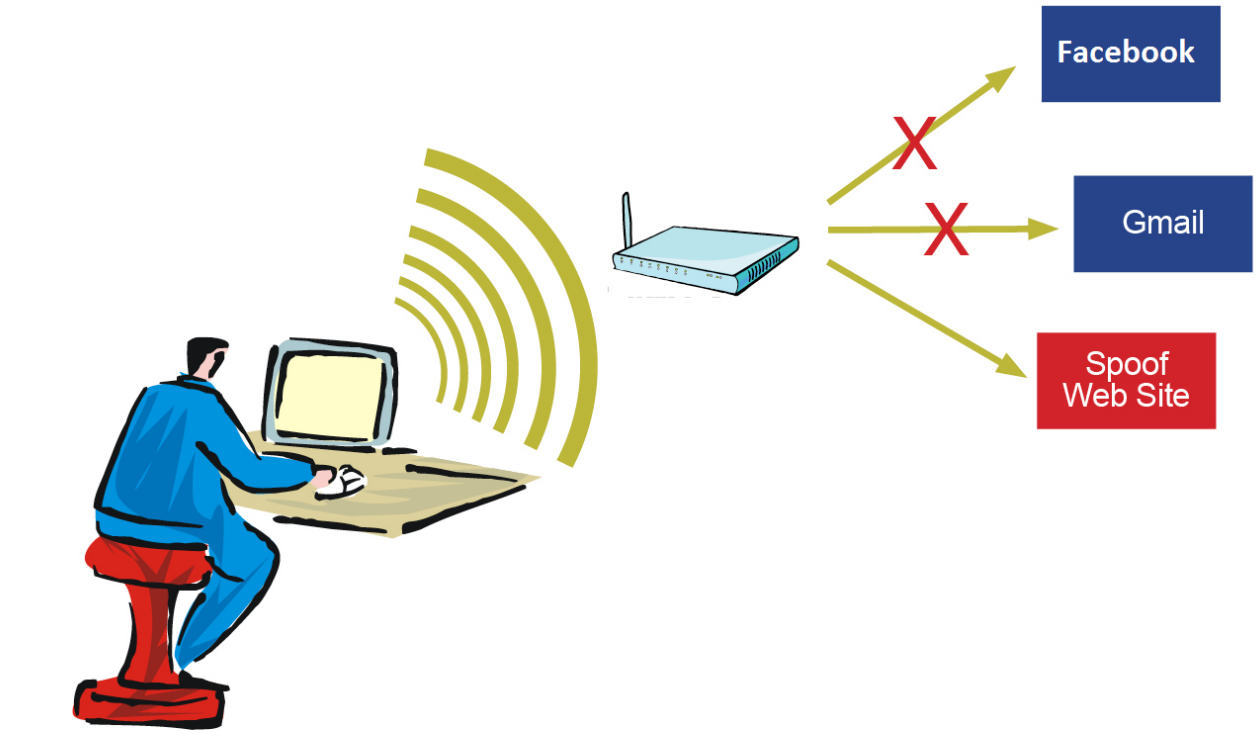
In a pharming attack, hackers redirect traffic from a genuine site to their own website, in order to collect information or credit card numbers from users. Pharming is a risk when connecting through either a wireless or a non-wireless connection.

Remember that in a phishing attack, hackers will make a fake website that looks like the real one—for example, a site for a popular bank. Then, they lure users to the site through a scam email. But users can avoid this attack by finding the proper URL for the genuine website and typing it into the navigation bar at the top of the browser window.

In a pharming attack, hackers can even send this direct traffic to their own site by hacking the real website's code to forward traffic. Or, the hackers can do a "drive-by attack," reconfiguring a wireless router. This is called "drive-by pharming" because the hackers can sit at the edge of a wireless hotspot—for example, in their car outside a coffee shop or an apartment building—and reconfigure the wireless router so that it sends all traffic to the hackers' website.

The best way to protect against pharming is to change the default ID, network encryption, and passwords on a wireless router, so that hackers can't reconfigure it.

PHARMING



WIRELESS USER