**Internet security**

**How to Secure Your Home Network**

We've been treated to some pretty entertaining feats of espionage courtesy of Hollywood. Who can forget the way Tom Cruise dangled from the ceiling as he attempted to crack into a computer security system in "Mission Impossible?" or how about the mysterious hacker who seems to slip past every security to corrupt the Rossum Corporation's data in the "Dollhouse" television series? Hacking into a network must require superhuman skills and knowledge, right?

You might be surprised to learn how easy it is for someone to hack into a computer network. The fact is that many computer networks are practically defenseless to intruders. In the early days of home computer networks, the people who put the networks together were experts and enthusiasts. They put their systems together knowing how computers can communicate with each other and built in protective measures to prevent other computer users from snooping.

Today, home computer networks are popular among a broad range of consumers. User knowledge spans from expert to newbie. Some users may be unaware of the dangers they can encounter if they don't properly secure their network. Others may think home network security is too complicated or confusing. But network security is more important than ever and it's worth the effort to learn more about it.

An unprotected network could allow malicious hackers -- known as crackers -- access to your data. It might even allow someone to take control of your computers and use them to commit crimes like a distributed denial of service attack (DDoS). Even if no one snoops on your information or controls your computer, someone might use your network to access the Internet. As more ISPs begin to place caps on how much data you can download, it becomes even more important to control your network. You don't want to get slapped with a huge bill for Internet services you didn't even use.

With the right tools and knowledge, you can minimize your chances of having your security compromised by malicious hackers or computer viruses. Let's get started.

When we talk about home networks, we generally mean a system composed of at least two devices connected to each other. Usually, these devices also connect to the Internet. Technically, if you have only one device connected to the Internet, it's part of a larger network. But you wouldn't have a network of your own.

Computers running on the Windows operating system are more at risk of security invasions than Mac computers. That's to be expected -- the Windows operating system dominates the computer market. That means the Windows platform is a big target for people who want to exploit computers -- they've got a much larger target and potential payoff.

Other devices that can comprise a home network include routers, firewalls, cable or DSL modems, printers, video game consoles, smartphones and voice over Internet protocol (VoIP) phones. Depending upon the protocols you use, you may have even more devices linked to your network. For example, Bluetooth gadgets can sync with each other when they come within range of the network.

From a security standpoint, the pieces of hardware that will help provide security are firewalls and routers. Firewalls come in two varieties: hardware and software. You can purchase a physical firewall device or run a firewall application. Many routers have firewall software built into them.

Firewalls act like filters. They help you monitor data traffic between your network and the Internet. If you detect unusual traffic, that's a potential sign that someone has compromised your home network's security. Most firewalls have several security settings to choose from. The most restrictive settings are generally the safest, but they also limit your options. Most firewalls will allow you to create a list of Web addresses that are off limits.

If you use a wireless router, you should make sure you set a password and enable encryption. Unprotected wireless networks are a bad idea. Most routers have either Wireless Encryption (WEP) or Wi-Fi Protected Access (WPA) encryption options. Some have both. WPA is more secure than WEP. Enabling encryption and choosing a strong router administrator password are two steps that will help keep your network secure.

On the software side of the security issue are several important applications. As we mentioned earlier, firewalls come in both hardware and software varieties. If you don't have a hardware firewall, you can use a firewall application to help protect your network. You can even use both a hardware and software version if you like.

There are several firewall programs available on the market. Some of them are free. Many are part of a larger software package that includes other important applications.

Almost as important as a firewall is anti-virus software. While you may be able to avoid most computer viruses, Trojans and other forms of malware through careful Web surfing habits, the truth is sometimes things slip through. All it takes is one mistake and you'll end up with an infected computer. A robust anti-virus program can help keep your computer safe.

Anti-virus software isolates and neutralizes malware. Most anti-virus software searches for viruses by comparing the applications on your computer against a huge database of malware. If something matches, the software alerts the user and attempts to neutralize the program. For anti-virus software to remain effective, it's important that you keep it up to date. Many programs have an auto-update feature that will download new virus definitions on a weekly basis.

Other useful applications to look into are anti-spyware or anti-adware programs. Like anti-virus software, these programs search your computer for applications that can affect your network's security. Spyware and adware can track your online activities and send information to another computer.

Many of these programs have active scan modes that will help you keep an eye on your computer in real time. Others may require you to set up a scanning schedule or run a scan manually. It's a good idea to run scans on a regular basis -- at least once a week.

A strong firewall should help you keep an eye on attempts to contact your computer. It should also alert you if an application on your machine is attempting to contact another computer. Keep a close eye on these messages. Some are harmless or even beneficial -- you wouldn't want to block your anti-virus program from downloading the latest updates. But others can be signs that someone is trying to access your information or control your machine from a remote location.

Most Web browsers have security settings that can help you keep your network safe. Several will warn you if you are about to visit a site known to host malware. You can also adjust settings such as whether or not your browser will accept cookies or run Java applications. Disabling cookies, Java and other options will help keep your network safe but it will also affect your browsing experience. You may not be able to interact with sites the way the webmaster intended if you turn off these options.

Administrators of commercial computer networks sometimes rely on special software and hardware called intrusion detection systems (IDS). These systems monitor data traffic across host computers and networks. A good IDS can compare this data against known malware patterns and alert the administrator if there's a problem. But that's a solution for a much larger computer network than your typical home network.

Most anti-virus software won't detect an intruder. But you might discover a malware application that makes intrusions possible. Run anti-virus software frequently to make sure your system is safe. You should also be sure to install updates and patches for your operating system as they become available. These patches may help seal up vulnerabilities on your computer.

Setting up a secure network is one thing -- keeping it secure is another. All your hard work will go to waste if you aren't careful about how you use the Internet. But if you follow a few guidelines, you'll greatly reduce your chances of compromising your network's security.

The first tip is to avoid clicking on hyperlinks in e-mail or instant messages, particularly if you don't recognize the name of the person sending it to you. The link may lead you to a site hosting malware. It might even initiate a malware download. Tell your friends and family that you avoid clicking on hyperlinks unless you are sure they lead to a safe destination.

Sometimes links on Web pages can also lead to malware. You might click on a link thinking you're going to one site when you're really going to another. Some malware designers will go so far as to create a copy of a legitimate Web page and use it to host their malware. It's called spoofing. Fortunately, it's not that common -- most legitimate sites are quick to take action when they discover a spoofed version.

If you want to make sure you're visiting the right Web site, you shouldn't rely on hyperlinks at all. The most reliable way to reach the site you want is to type the URL into your browser's address bar. Even this method isn't completely foolproof, but it's the most reliable way to make sure you go to the site you want to visit.