7 Tips for Building a Secure Home Network

1. Make sure to install virus protection software on all PCs on your network, and make sure they are updated as routinely as possible.

2. Enable Microsoft file and printer sharing with extreme caution. If you set permissions incorrectly, outsiders can locate your PCs more easily and gain access to files on your hard drives. Consider enabling port blocking on your firewall.

3. If you have children using your network, consider setting up some form of Web filtering through either a software-based firewall or a hardware firewall.

4. If you choose a hardware firewall, make sure it includes Stateful Packet Inspection (SPI). SPI inspects the content of packets to determine where to allow them access to your network.

5. If you're building a wireless network, be sure to turn on WEP (Wired Equivalent Privacy) on your wireless router or access point.

6. Periodically check for heavy traffic on your router's LEDs and whether each PC's log files contain new entries you are unfamiliar with. These factors could indicate that someone has hijacked your PC and is using it for DdoS attacks or other malicious activities.

7. At night, shut off your wireless router – especially if you live in a densely populated area – and your PCs. What is not available cannot be hacked.