Internet Security

Internet security has 3 lines of defense:

ISP - provides anti-virus, spam and content filters

Hardware router - You provide firewall, IP Filters and protocol filters

Software - You provide firewall, anti-virus, anti-trojan, anti-spyware, anti-spam, privacy filters, ad blockers, popup blockers and e-mail encryption

Hardware:

Linksys network interface card - LNE100TX	$15
Linksys Router (single port) - BEFSR11	$40
Linksys Router (4-port) - BEFSR41	$45
D-Link Router (4-port) - DI-604	$34

Software:

Zone Labs - ZoneAlarm firewall - basic level free for personal use
Symantec - Norton Anti-Virus $40 - $50 + $20 rebate
Grisoft.com AVG anti-virus - free for personal use

Mozilla (free) browser provides managers for:

- Cookies
- Images
- Popups
- Forms
- Passwords
- SSL
- Certificates

Mischel Internet Security - TrojanHunter $40 or free 30-day trial www.misec.net

PestPatrol.com - free for detection only. $40/yr for cleaning tool

Identity theft - via the Internet

1) Do not send sensitive information via e-mail
2) Shop the Internet with companies you know. Check their identity. Ensure transactions are encrypted.
3) Do not use Debit Cards for Internet purchases
4) Never give out passwords. Change them often. Do not use real words.
5) Monitor your credit reports
6) Be leery of sites that ask for sensitive information. Don't provide it unless they really need it.

GLOSSARY

Ad blocker	Software placed on a user's personal computer that prevents advertisements from being displayed on the Web. Benefits of an ad blocker include the ability of Web pages to load faster and the prevention of user tracking by ad networks.
Content filter	Removes potentially harmful or undesirable material from a message. Typically used for blocking porn.
cookie	A small text file that is placed on a user's hard drive by the Web site that the user is visiting. This file records preferences and other data about your visit to that particular site. This is most evident when a user returns to a site and is greeted by name. Cookies are often used for long term data collection.
encryption	The scrambling of digital information so that it is unreadable to the average user. A computer must have "digital keys" to unscramble and read the information.
firewall	A hardware or software device that controls access to computers on a Local Area Network (LAN). It examines all traffic routed between the two networks – inbound and outbound – to see if it meets certain criteria. If it does it is routed between the networks, otherwise it is stopped. It can also manage public access to private networked resources such as host applications.
IP filter	An IP address is a number or series of numbers that identify a computer linked to the Internet. As a general rule, the IP address is written as four numbers separated by periods. For example: 12.24.36.48. An IP filter can be used to block an individual address or a block of addresses.
popup	A new browser window that appears unrequested (by you) on your screen. A gratuitous, easily-programmed visual effect exploited by many web sites often to the consternation of the hapless user. Commonly used for advertisements. Particularly annoying are those termed exit popups: browser windows that spring to life when you leave a site or when you close a browser window. (Scripting languages call these "onUnload" and "onClose" events.)
Privacy filter	Secures private information about you from access by unauthorized individuals or organizations. May be used locally to encrypt and/or remove data from common system files.
Protocol filter	Software or hardware that screens network traffic for a certain protocol, and determines whether to forward or discard that traffic based on the established criteria.
Spam	Spam is the common term for unsolicited e-mail.
spyware	Hidden software (supposedly) surreptitiously installed on your computer that collects information and sends it to the author/organization.

trojan	This describes a computer program that appears to be something useful, but then does something malicious to your computer. This could range from destroying data to laying dormant and someday hijacking your computer to be used as part of a denial of service attack. Anti-virus programs will protect you from known Trojan horses, but strictly speaking, Trojan horses are unlike viruses as they do not replicate. However, combination virus / Trojan horses can replicate.
Virus	A program that makes unbidden copies of itself. Sometimes these copies are added on to executable files, and other times they are part of Word or Excel documents, called Macro Viruses. The virus will usually have some eventual effect on systems that are infected. Often, the intent of a virus is malicious. Sometimes the intent is not malicious, but due to the spreading of the virus, it becomes a malicious act.