

INTERNET SAFETY TIPS

- **Use a Firewall** - A firewall is a piece of software or hardware that sits between your computer and the internet and only allows certain types of things to cross the wall.
- **Virus Scan** - Sometimes, typically via email, virii are able to cross the wall and end up on your computer anyway. A virus scanner will locate and remove them from your hard disk. A *real time* virus scanner will notice them as they arrive, even before they hit the disk, but at the cost of slowing down your machine a little. **Important:** because new virii are arriving every day, it's important to keep your virus definitions up-to-date. Be sure to enable the scanning software's automatic-update feature and have it do so *every day*
- **Kill Spyware** - Spyware is similar to virii in that they arrive unexpected and unannounced and proceed to do something undesired. Normally spyware is relatively benign from a safety perspective, but it can violate your privacy by tracking the web sites you visit, or add "features" to your system that you didn't ask for.
- **Stay Up-To-Date** - Over 90% of virus infections *don't have to happen*. Software vulnerabilities that the viruses exploit usually already have patches available by the time the virus reaches a computer. The problem? The user simply failed to install the latest patches and updates that would have prevented the infection in the first place..
- **Get Educated** - Don't open attachments that you aren't *positive* are ok. Don't fall for phishing scams. Don't click on links in email that you aren't *positive* are safe. Don't install "free" software without checking it out first. •

It all might seem overwhelming, but it's not nearly as overwhelming as an actual security problem if and when it happens to you. While we might want it to be otherwise, the practical reality of the internet, and computing today, is that we each must take responsibility for our own security online.