

Internet Security



Securing Your Network

The Internet is one huge network comprised of computer users all around the world that exchange all types of information. As Internet use has exploded in the past few years' businesses and consumers have found new ways to harness its ability to share information. For example, you can email or instant message with your friends, work from home and connect to your corporate network, or you might purchase a book from Amazon. The information relayed with each of these activities varies in its sensitivity and thus corresponds to the extent that you would like to protect and secure that information so that others cannot observe it.

When we consider information security, we recommend that you start with the assumption that all of your Internet traffic could be observed by others unless you take appropriate precautions that will protect your data and ensure that others will not be able to observe your information. This guide is meant to provide you some background on different types of security and when they should be used.

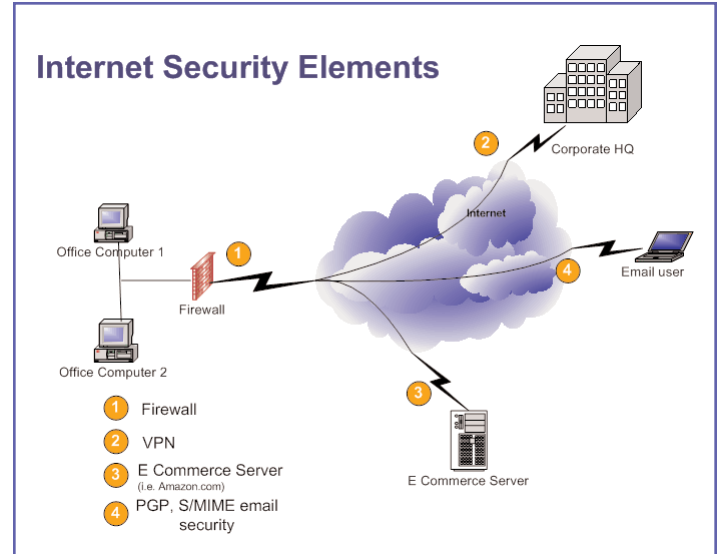
Strategies to Consider

VPN (Virtual Private Network) - A VPN is a method to protect information transfer between two parties that communicate across the Internet. Generally, a VPN is used when the same two parties exchange information frequently- i.e. several times per week. To complete a VPN, two things must happen. First, each party must demonstrate or authenticate to the other party who they are. Next, the data is secured by encryption as it is exchanged between the two parties. Encryption is the process of taking data information and jumbling it with an algorithm so that others can't interpret it. Essentially, a VPN establishes a virtual tunnel between the parties. An example when a VPN might be used would be when someone wants to connect to his or her corporate network to work from home.

SSL (Secure Socket Layer) - SSL is another means used to encrypt communication between Internet users. Generally, it is used to enable a private exchange of information between users that share information infrequently, such as the transmission of credit card numbers for e-commerce or when connecting to an Intranet or Extranet. You may have experienced SSL when purchasing goods or services via the Internet.

Email Security - Two different methods, Pretty Good Privacy (PGP) and Secure/Multipurpose Internet Mail Extensions (S/MIME) enable you to secure email communication. Both methods authenticate or confirm the identity of each party to the email and also to protect the integrity of the message through encryption or other comparable means. Generally, all email programs will support one of these two standards if configured properly. Prairie iNet supports both of these protocols, but you must configure you email client software program, such as Microsoft's Outlook or Outlook Express, to utilize the protocols.

Microsoft Windows security - With the introduction of Windows 2000 and XP, Microsoft made enhancements in the ability to secure IP traffic. Review IP security within the Help section of Windows for more information.



Firewall - A firewall is hardware or software component that observes and monitors all information that comes into and goes out of a network. As it monitors traffic it can perform several tasks including, watch for and prevent unwanted users from accessing or "hacking" into your network, prevent outgoing users from visiting certain web sites such as pornographic and sports web sites while at work, and monitor how people use the Internet by tracking viewing habits of individual users monitoring such things as most visited web sites and the amount of time individuals spent accessing information at each web site.

Viruses - A computer virus is a mini program designed to replicate and spread, generally without the user's knowledge. Viruses spread by attaching themselves to other programs or files on a hard drive. When an infected file is activated or executed, or when a computer is booted up, the virus itself is also executed or activated. Generally, viruses penetrate a network via an email attachment, but they also may enter a network through a download, or less frequently, via general web browsing. Anti-virus software programs perform three functions, including detecting, identifying, and removing viruses.

As you weigh different hardware and software solutions to secure your Internet information, be aware there can be significant differences in the features offered by the hardware and software solutions for each strategy. We advise you to work with your computer integrator to develop a strategy catered to the needs of your organization.

For additional information, please visit the following web sites:

Microsoft - www.microsoft.com/security

Symantec - www.symantec.com

Sonicwall - www.sonicwall.com

Checkpoint - www.checkpoint.com