Since you're reading this article, you're already connected to the Internet. You've probably already thought about security on your computer or network. Every day seems to bring new threats and it can seem pretty daunting, but the key thing is to have a common sense approach and to take a few basic precautions.

There are lots of great tools available to help and you don't have to break the bank to get them. Here are some areas to take a look at:

BACKUPS

Securing your information starts here. You'll need some or all of the security tools listed below, but even then you can't guarantee 100% that you won't have a problem. Hardware failures do occur so backup your data. One easy way to keep your important files is to burn them onto CD or DVD.

ANTIVIRUS SOFTWARE

An absolute must have. Alright, you already knew that, but I can't stress too strongly the importance of having good, up-to-date antivirus software. With new threats and Viruses arriving every day it's important to maintain update subscriptions and download virus definition updates as soon as they become available.

There's a lot of good antivirus software available, both free and for low cost. I'd recommend going for paid software...you just never know when you're going to need to call a helpdesk and that's generally the difference between the free stuff and the stuff you pay for. Norton, McAfee, AVG and others all sell antivirus software that's affordable on a low budget.

FIREWALL

A firewall is always recommended to help protect against unauthorized access to your PC. For a small number of PCs a software firewall is usually best and is the easiest to work with if you're not an IT expert. However, don't discount hardware firewalls, especially if you have a network with a lot of devices on it.

Whatever you do, don't rely on the Network Address Translation or packet filter built in to your ADSL or Cable router. It almost certainly won't be enough.

If you're buying a particular company's Antivirus software it's worth considering buying their integrated AV and firewall package if they have one (if they don't then maybe you should try someone else). It may well save you money and be easier to configure and maintain.

ANTI-SPYWARE SOFTWARE

If you spend a lot of time browsing the Web (and let's face it, who doesn't?), then spyware is going to find its way onto your machine. A lot of it isn't particularly nasty, but the really bad stuff can send important information like passwords, bank details or credit card numbers to people you really don't want to have access to that stuff. At the very least it can slow down your PC and since you didn't ask for it in the first place then you should get rid of it.

Some tell-tail signs that you have a Spyware infection are:

- You're getting pop-up ads all the time

- Your default homepage or other settings in your browser suddenly change (especially if you can't change them back)

- Your computer is slow (there could be other reasons for this, but it's worth checking for spyware)

There's some good free software available from Lavasoft called AdAware. Microsoft also have their own free tool for Windows users called Windows Defender. Among the paid-for Anti-Spyware software Webroot's

Spy Sweeper regularly picks up awards from computer magazines.

PASSWORDS

More and more people are accessing secure sites for shopping, banking, etc. Provided you take sensible precautions it's a great way to shop.

If you've been doing any online shopping you'll be used to dealing with secure sites.

Whatever methods these sites use to secure their servers or encrypt your traffic, if they're accessed by passwords then you share some of the responsibility for the security on your transactions. Here are a few tips on how to keep unauthorised users from accessing your accounts:

- Be inventive with your passwords. Don't use easy to guess stuff that a lot of people know about you or can find out. Use a mixture of uppercase and lowercase characters, numbers and special characters (again be inventive. Just using a 1 instead of the letter i is no use if it still spells out an easy to guess word).

- Use different passwords for different accounts. If you always use the same one and it's compromised then someone will have access to everything.

- Don't write passwords down on paper or post-it notes. That's a hacker's favourite way to find passwords if they have physical access to your office.

- Don't get Web browsers to remember your passwords on shared machines or in office areas. If you log into a machine that other users have access to then never use Windows or Web browser mechanisms that remember your account details.

Having different passwords to lots of different accounts does make it more difficult to remember them and it's important that this doesn't lead you into bad habits. So what do you do?

You could look at getting some password management software. Naturally, Norton has a password manager, but other good options include "Web Replay" from Deskperience or "PC Password Manager XP" from CPLab.

WHERE TO NOW?

You don't have to go out and buy every piece of security software right away. Prioritise one or two to start with (I'd suggest Antivirus and Firewall software). Also download trial versions so you can be sure you're happy with them before you part with your hard earned cash.

Be careful on the Internet, but don't let it spoil your day.

Russell Card has been an IT Consultant for over 10 years and has extensive knowledge and experience in Networking, Security, Web Design and a host of other computer subjects. To find more articles like this, visit UKITbits

Article Source: http://www.articlecube.com