Protecting Yourself Online

Every day a number of new and malicious programs are released onto the Internet. The purpose of these programs ranges from finding out your most visited sites and tailoring annoying pop up adverts to suit, through to gaining your personal details for use in identity theft. As each new program is released, the various methods employed to steal your information or defraud you are becoming more and more sophisticated.

Luckily for us, the methods for protecting ourselves online are just as effective.

The following is a brief introduction on how to protect yourself when using Accessweb and the Internet in general. This will hopefully prevent any loss of data, be it financial, personal or otherwise.

It starts with you!

First and foremost, YOU are the best protection you have on the Internet.

Being "hacked" is not as easy as it is made out to be, and there is a level of user interaction required before a "hacker" will be able to gain access to your system. This could be as much as downloading and installing a program or as little as clicking on a link within an email.

Here are some simple things you can do to aid in your own Internet security:

- Do not use Internet Banking from a public Cyber Cafe. You have no control over the security of the machines or the person who logs on next.
- When at home, do not click on links you receive via email from people you do not know. Always verify the address and be especially careful if it is offering something for free or asking you to download a program.
- Some emails purport that you can receive millions of dollars for free if you give the sender your bank account number and personal details. This is commonly known as a "Nigerian Bank Scam" and is just that, a scam. "Free" on the Internet is dubious at best.
- Never write down or tell anyone your Account Password. Treat this the same as you would a PIN number - MEMORISE IT and keep it secret. Make sure you select a password that is difficult to guess and change it regularly.
- Your Credit Union will NEVER email you asking for your Account Number or Password. If you receive an email like this, DO NOT reply to it or click on any of the links on offer.
- Never leave your computer logged on to the Internet when you are not around and always log out when you have finished your online banking session.
- When you are surfing the Internet, be wary of pop ups asking that you download a program or click on a link for no apparent reason. Do not click on the "Ok" or "Cancel" buttons as these generally both "accept" the download. Look for the red cross at the top right of the window and click that to close the window instead.
- If you do download programs from the Internet regularly, make sure they pass a virus scanner check before installing (see the next section)

Useful security tools

Following the above guidelines will go a long way in keeping your computer secure and free from viruses and Spyware.

In this section, we will go through some useful tools to further add to your computer's security.

Virus Scanners

A good Virus scanner is the first thing you should get for your computer if you do not already have one.

These programs will sit active in the background when your computer is switched on and monitor your system constantly for viruses. This includes anything you may inadvertently download and things that try to download and install themselves without your knowledge.

A Virus Scanner is only as good as its current virus database, so these must be kept up to date to ensure that your virus scanner is working at its optimum level. Most virus scanners have a schedule that you can set, which will download and install all updates for your virus scanner automatically.

Firewalls

Personal firewalls are common as a means of protection from intruders on the Internet. Think of them as a large door that will only open for people you specify and will stay closed and locked to all others.

If you have Windows 7 or Windows Vista, a personal firewall is included by default. If you have WindowsXP and have kept it updated, you would have received a Personal Firewall when you upgraded to Service Pack 2.

There are several companies who offer "Internet Security" suites. These are software packages that contain both antivirus and firewall components, among other features. The advantage of these products is that you only have to install and update one program to take care of your Anti Virus and Firewall needs. Most of these suites also include Anti Spam tools for your email and Anti Spyware tools for web browsing as well as phone and email support for any problems encountered.

Some popular security suites for Windows include:

- Symantec - www.symantec.com/
- McAffee - http://us.mcafee.com/
- TrendMicro - http://shop.trendmicro.co.nz/

There are less options for security packages for Apple systems, but there are a few options available:

- ClamXav - http://www.clamxav.com
- SecureMac - http://securemac.macscan.com
- Virus Barrier - http://www.intego.com/virusbarrier/

Spyware removal

Spyware programs typically install themselves on your computer either by way of you clicking on a link or without your knowledge when you visit a Spyware website.

These programs do anything from changing your homepage and redirecting you to "questionable" websites, capturing your surfing data and selling it on to advertising companies, even installing "key logging" programs that log your key strokes and send these back to the Spyware author, giving them things like Internet Banking logins and passwords and more.

If you suspect you have been infected with Spyware, there are 2 free tools that are excellent for detectin g and removing most Spyware programs:

- **AdAware - http://www.lavasoftusa.com/**
- **Spybot Search and Destroy - http://www.safer-networking.org/en/index.html/**

Like the Anti Virus programs, Spyware removal tools are only as effective as their Spyware database is, so it is important to keep these up to date to ensure maximum coverage when searching out Spyware on your computer.

The programs above, used and updated properly, will help greatly in keeping your computer secure and safe whilst you are online, reducing the risk of you becoming the victim of an online attack.

However, these do not offer a 100% guarantee of security. As noted in the first section, a lot of the decisions you make whilst on the Internet will dictate how effective these programs will be.

In using the same analogy as the Firewall section, if you think of all these programs as being a large metal door to your house, then it will certainly provide you with adequate protection when locked and closed, but if you unlock and open the door to the wrong person, it will effectively make the door useless.