A beginners guide in how to make a Laptop/PC more secure.

This guide will go through the common ways that a user can make their computer more secure.

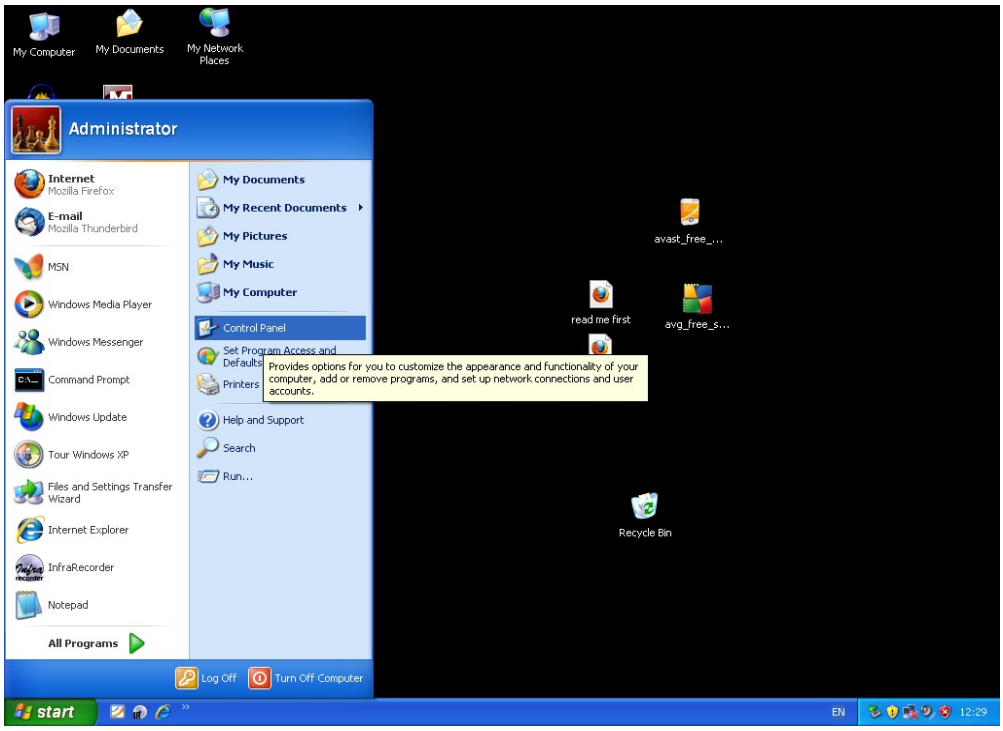
Here are the key points covered:

1) Device Password
2) Anti Virus, Firewalls & Updates
3) Changing Passwords & Saving Passwords
4) WEP/WPA & Use Of Public WI-FI Hotspots
5) Backing Up Data
6) Encryption
7) Email Security
8) PGP

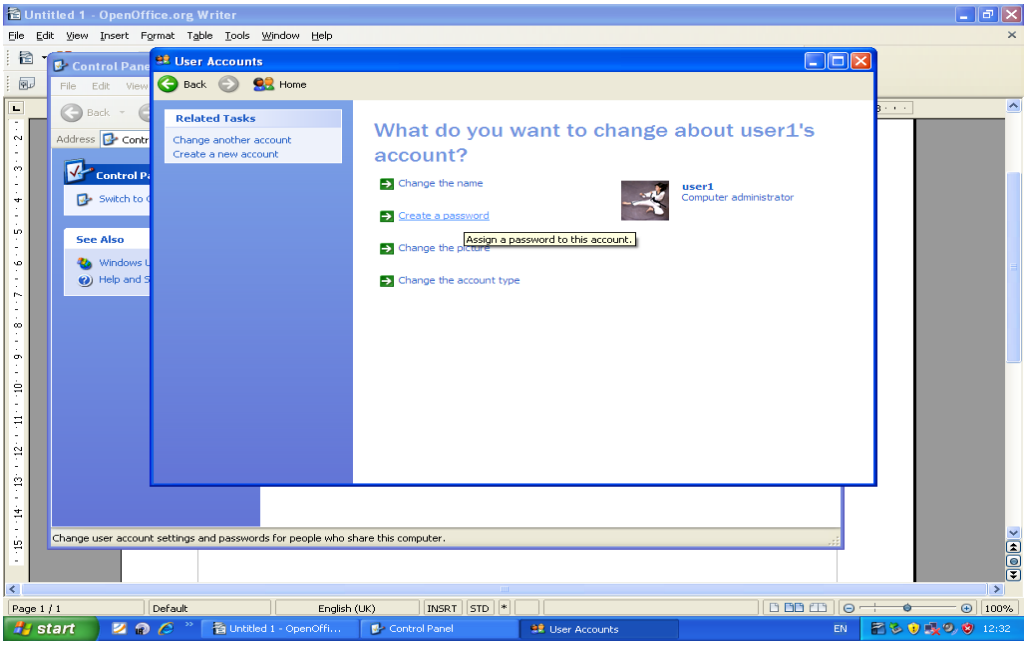
Device Password (1)

A device as in a computer, laptop mobile phone can be password protected. This means that the device will be locked until a unique set of digits that were set by the user is entered. Although there are ways to break this small step it is still an essential first step in security and an easy step to take. Also note that you can make separate accounts for users and have one administrator account for the owner of the computer. This is a great way to keep your documents private from another user of the computer/laptop. The screen shots will go through in how to set a password using Microsoft Windows XP. Different systems have slightly different ways to do this.

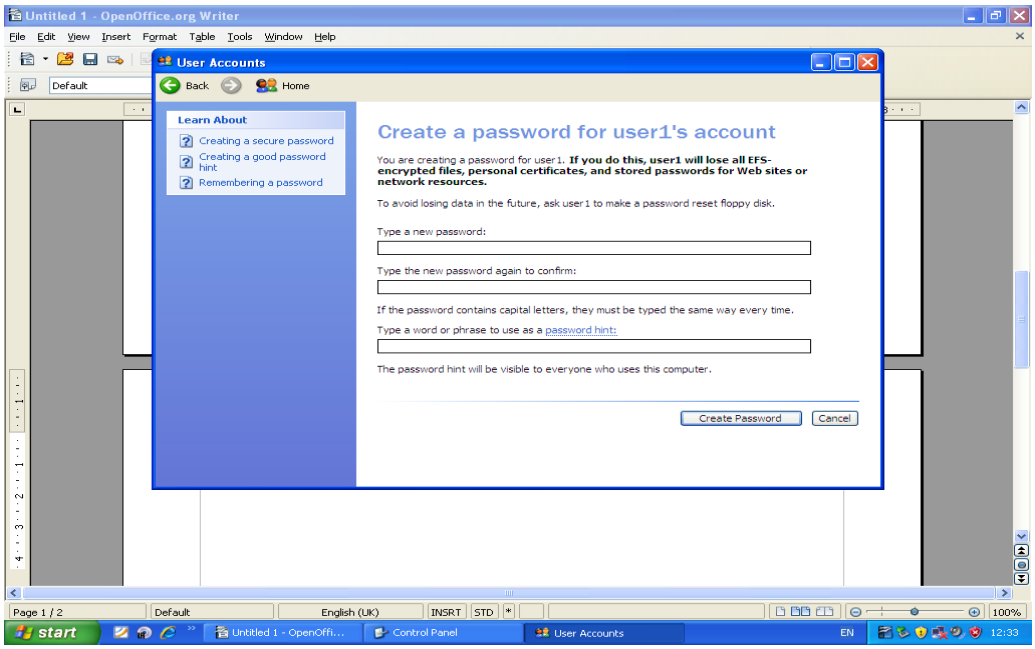
Step 1:
Go to start then click on Control Panel



Step 2:
Once the window called control panel has loaded click on icon called 'User Accounts' which is usually at the bottom. Once you do that a new window called 'User Accounts' will appear on the screen. Click on the account that you want to create a password for. In this case it would be 'User 1' as I have already created a password for the administrator. If your computer has not yet had any passwords then you will have only 2 options which will be administrator or guest. If that is the case then click on Administrator. Once you have done that the windows will Change and you will get more options. Click on the second option which says 'Create a password'.



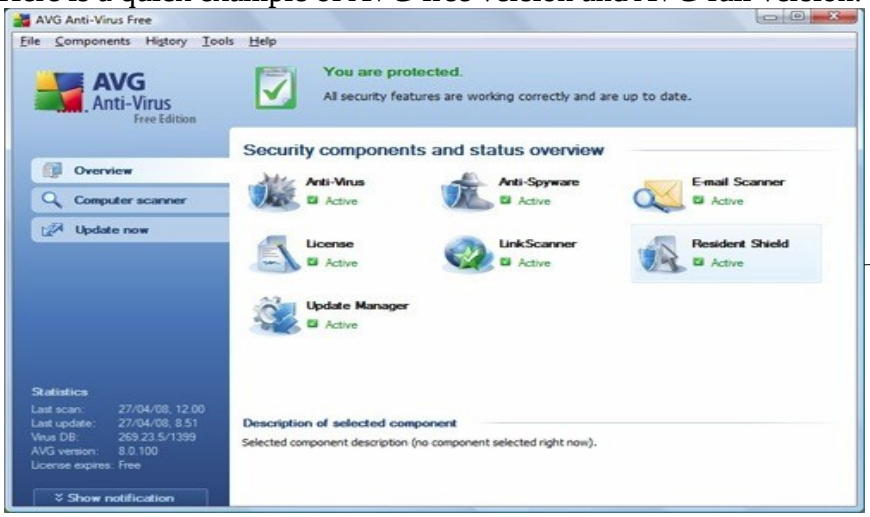
When that is done the window will change once more and you will be able to enter specific information. Now remember to choose a password that you would remember. Type it in the first box called 'Type a new Password' then type it again to confirm it in the box called 'Type the new password again to confirm'. You may also add a hint to that password to help you remember it. So if I had a password that was associated with my date of birth I might put June. This is not a must but it will help you if you need it. Once you have done that click on the button at the bottom that says 'Create Password'



Anti Virus, Firewalls & Updates (2)

In Simple terms Anti Virus is software used to prevent, detect, and remove malware, including computer viruses, worms, and trojan horses. These programs may also prevent and remove adware, spyware, and other forms of malware.
A firewall in simple terms is part of a network that is designed to block unauthorised access while permitting authorised communications such as going online using the internet. It is a device that is set to allow or deny computer applications depending on the setting that you have set. When you purchase a computer or laptop you must note that unless a subscription to anti virus software is part of your purchase you have to buy one. Now there are many ups and downs on different types of anti virus software but whatever they are they still have the same job in mind which is to protect your computer. From the above threats. I recommend 2 free based anti virus software which are AVG and Avast that you don't have to pay for but you may pay for extended features. Remember that only a home user is licensed to use the free version of AVG and Avast.

Here is a quick example of AVG free version and AVG full version:



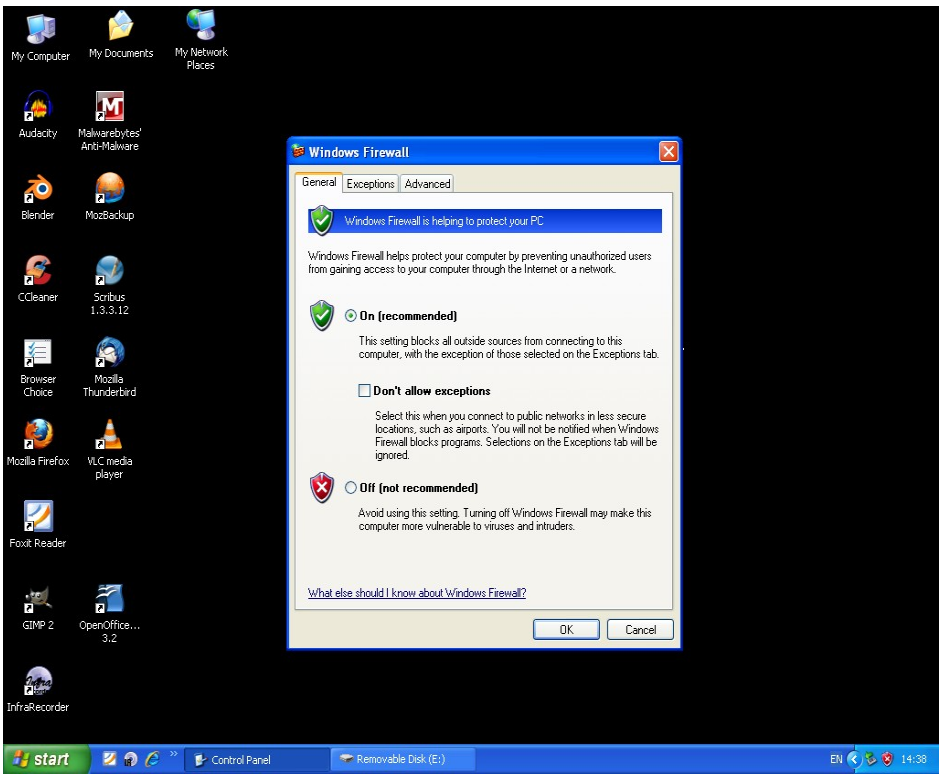
This is the free version of AVG.

Here is the full version which has more features that are available.

for more information you can go to http://www.avg.com/gb-en/homepage
For more information on Avast you can go to http://www.avast.com/en-gb/index

Now to firewalls. Microsoft Windows has a firewall that comes with the system itself. There are operating systems such as Linux which do not have a built in firewall and so you may have to look for software that are able to provide that need. I also will mention that most paid versions of anti virus software comes bundled in with a firewall too as you can see on the above screen shot of AVG full version. It is very important that whichever firewall you are using you turn it on especially when you are going online. If you turn it off to perform maintenance you must remember to turn it back on after. Here are steps to make sure that windows firewall is functioning.

Step 1
Go to start then click on control panel. When the window called 'Control Panel' appears on the screen double click on 'Windows Firewall'. When that window comes up make sure that the first option called 'On (recommended) is selected if not do it. Now there are other options that are available such as allowing a particular network connection services and applications. Make sure that the selected exceptions are that of use to you such as your Ethernet internet connection. When you are done you can now click on 'OK'.



Now another major point to take is updating your operating system, anti virus and any other security software with the latest patches from the manufacturers website. To do this in any system is not such a hard process. You may manually download updates or set your computer to automatically download updates or remind you to do it. If you do not want your computer or laptop to automatically download updates then remember to manually do so. In Windows you may go to the Microsoft update website. For a anti virus software you must do the updates too because new threats come out and your old definitions may not pick up new threats.

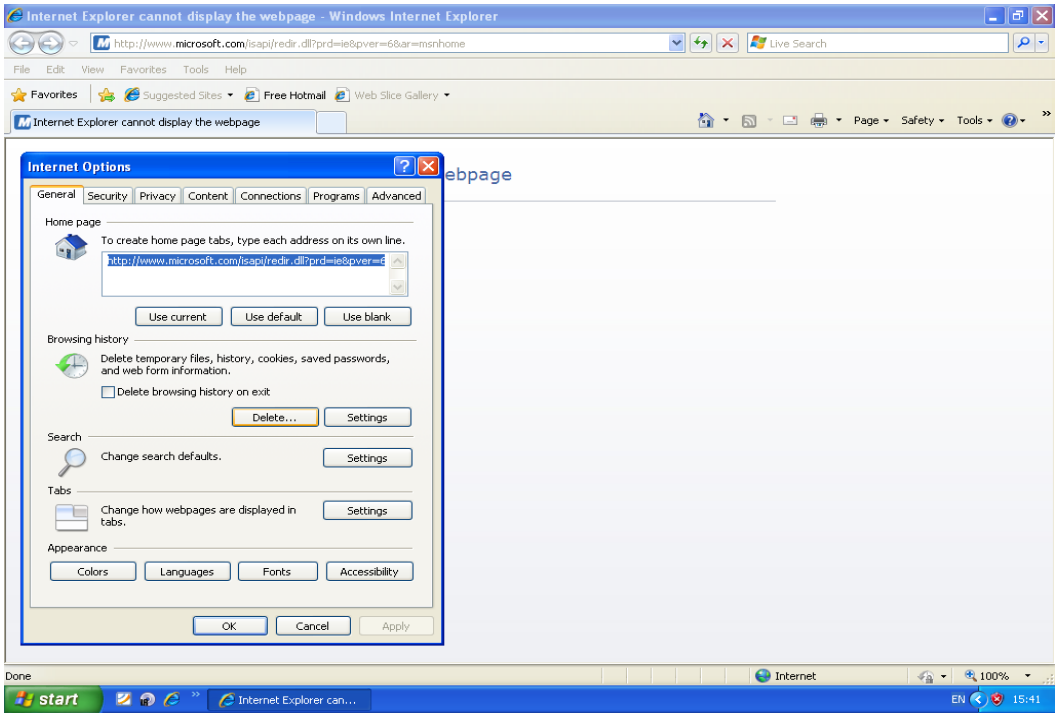
Windows update website is *windowsupdate.microsoft.com*

Changing Passwords & Saving Passwords

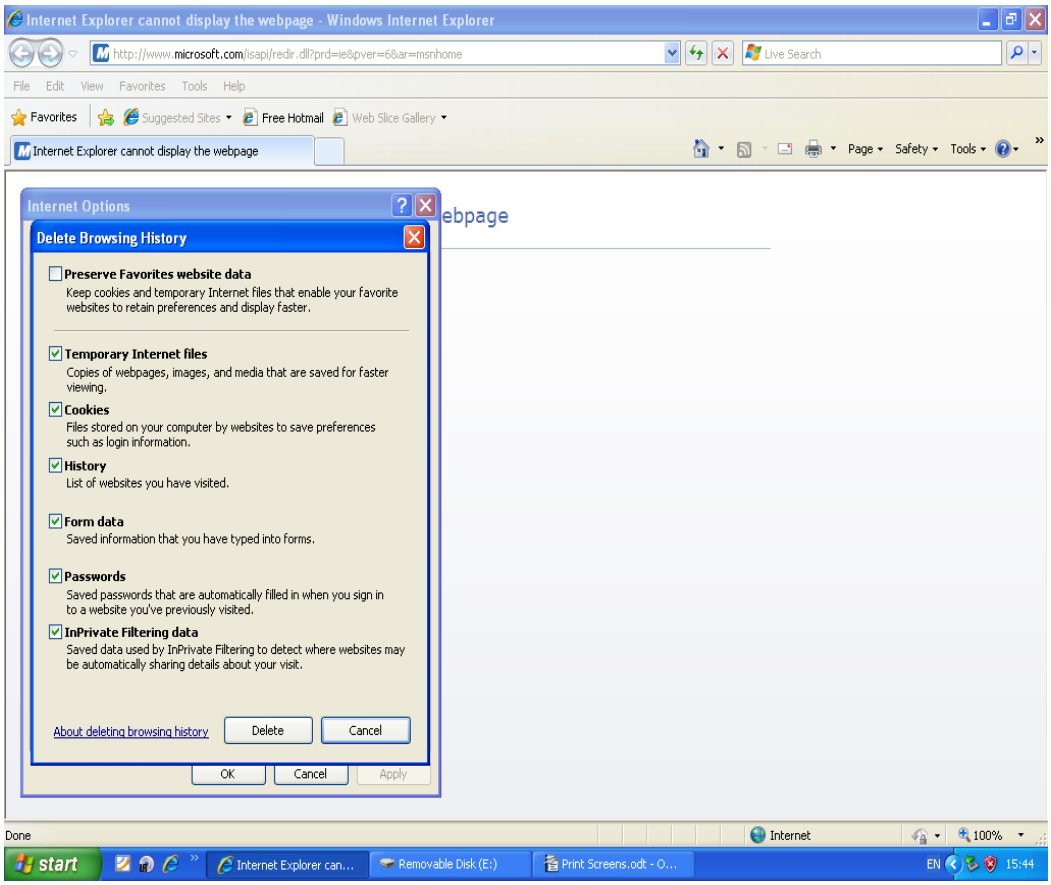
The reason why changing passwords is also an essential security measure is because lets face it but if someone really does somehow get the glint of your password using lets say a key logger or even watching physically and they have it or are getting close to getting it you may stop them with this simple step. Before they change it and take it over wouldn't it be better to change it yourself? If you change your password regularly although you don t have to do it every time you are much less likely to be a victim. The person may not even get a second chance. It is good to do this every 2 or less months or which ever is more comfortable to you. This goes for your device, hotmail and any other really important accounts you may have.

Another thing in this section is saving passwords. When you log on to a site such as hotmail your web browser has the ability to store your password so the next time you want to log onto your account you don't have to put in your password. Now there are advantages and disadvantages to this. The main advantage is that it saves you a little time and hassle in typing your password in every so often especially if your going to visit the website around 50 time a day. The main disadvantage is that this laptop or computer may not be in the right hands. Imagine for instance this was your hotmail account which usually acts as your master account for many other things such as paypal, e-bay etc. and so also holds account passwords and user names in some instances or even reset options and that you had your password saved . This means anyone with your laptop or computer also has access to your hotmail inbox which leads to the other accounts. So it is important that if you are going to set this option to remember passwords whilst your using the laptop or computer you may wish to delete them after you're finished. For example I work in an office and I take my laptop to work. Whilst I am on the laptop at work I may not turn this option on or even if I do I would lock the laptop if I leave it unattended for a minute and at the end of the day delete them. Below you will see how to delete passwords and cookies in Microsoft Internet Explorer & Firefox Web Browser.

Step 1 (Microsoft Internet Explorer)
For Microsoft Internet Explorer go to Tools, then click on Internet Options. When the window called 'Internet Options' Appears on the second option called 'Browsing history' click on the button that says 'Delete'.



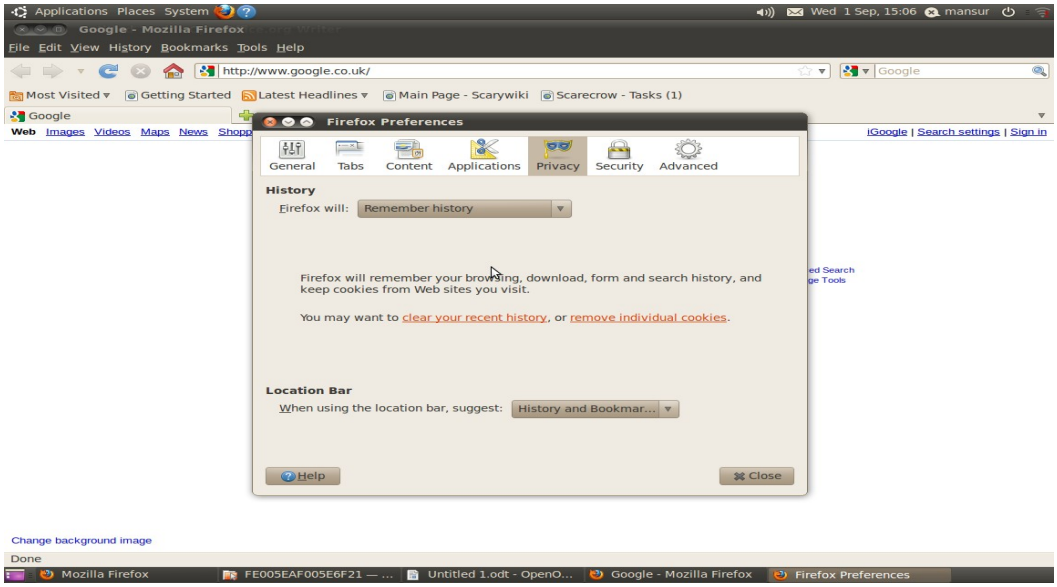
Step 2 (Microsoft Internet Explorer)



now on this screen tick the box called 'Password' you may tick or untick other boxes if it concerns you. Now click on 'Delete'.

(Firefox Web Browser)

Go to 'Edit' then click on 'Preferences'. A new window called 'Firefox Preferences' will appear on the screen. Go to the 5th tab which is called 'Privacy' and click on it. On the option called 'clear your recent history' click on it and confirm. When you are done click on 'Close'.



WEP/WPA & Use Of Public WI-FI Hotspots

If you have internet access at home or wherever you are staying it is usually nowadays wireless technology internet that allows broadband use. When you connect to the router (This is a little box that connects to the telephone wall socket and “routes” network access to the internet, often with wi-fi built in) you are asked for a security key which is usually WEP or WPA. This is a unique encryption key that is used to protect encode traffic routed. If you do not have your router protected with a key then anyone can access your signal unencoded. It is important to make sure that you have your router protected. When you subscribe to any internet service your ISP (Internet Service Provider) should give you a box that has protection enabled./ Remember to keep the key safe. Some see it as a public service to leave an open connection but be aware that in so doing others may use your ISP to their own ends. At it's most benign this might mean they steal bandwidth to make a large download and you notice things going slowly. At the worst case they might be downloading illegally and it is possible that, since the connection is your own your ISP may hold you liable (it would be very hard to prove otherwise).

Another important thing to note is that when you are out and about in any public place that offer free WIFI hotspots this connection could be insecure and in connecting your computer you could be putting your laptop or computer in risk. That is why it is really important to use firewall and anti virus software on your laptop or PC.

Backing Up Data

One of the most important aspects to computers is data back up. For instance imagine that you have really large and important files that have to meet demands and deadlines at certain times and that cannot be quickly recreated. Now having only the original version of this data is probably the most risky position to be in and yet a surprisingly common approach. Anything from a natural disaster (may be unlikely where you are but yes it can happen) such as a flood or a hard drive crash can result you in losing your valuable data. Whilst you may not care about it too much when there's a flood if it is just your computer on the blink you probably will .

There are a lot of ways in which you could back up your data. Backing up data is not at all difficult and can be done relatively quickly. I would recommend for a home user to purchase a USB Memory stick if there's not too much data that needs backing up or a portable hard drive if it is a lot of data that needs backing up regularly. These can be purchase quite cheaply nowadays and is a worthy investment. It is important that you back up your data on a regular basis.

Below are some sites that you can go to buy a USB Memory stick or portable hard drive online.

http://www.ebay.co.uk/

http://www.amazon.co.uk/

Encryption

In simple terms data encryption is a process in which plain text data is converted into ciphertext (encoded message) so that it cannot be read.

In this process, a piece of plain text which can be read by any person is converted so that it can only be read by a person with the key.

It is very important that if you carry documents with very sensitive data on them then you encrypt the data. Also note that many email programs and sites that handle personal information such as addresses and credit card details offer data encryption while sending and receiving which means emails cannot be read by third parties.

There are some free encryption software that can be used although it would not be as good as a paid version.

Here are some sites you can check for free encryption software:

http://www.truecrypt.org/

http://www.freebyte.com/security/

Here are some websites that you can check to purchase encryption software:

http://www.deslock.com/

http://www.pgp.com/

http://www.secureaction.com/

http://www.cypherix.co.uk/store.htm

Email Security:

Everyday people send and receive email as part of their daily lives. The reason being emails is a quick and simple way to get a message across rather than spending time and money for paper based messages such as post.

Now you might think that every email you send or receive is secure but you have to think again. In this age where electronic communications is getting more and more common it is also building a society for hackers who will be targeting more people.

Just like a credit card transaction, internet calls and other electronic means of communication email can be intercepted if you are not aware.

When you send a email you must note that it may be intercepted by any hacker and much more easier if you are using a unsecured WIFI hotspot.

There are simple measures that one could take to make their emails more secure and should it be intercepted it will not make use for the interceptor.

A common approach to this that I really recommend is that you take the following steps:

1) Write you message using office and save it.
2) Use a file encryption software to encrypt the files (don't try to use password protected zip files as they can easily be cracked). (PGP)
3) First send the encrypted file to the recipient.
4) Then send the password to that encrypted file.

When using services such as Hotmail and MSN you must be very careful and know the hazards that are involved. One of the most crucial of those is that when a friend of yours is hacked every contact of his or hers including you may get messages that are supposedly from your friend which is viral.

It may contain anything from a trojan, spyware e.t.c. In that way they can get you as well as your friend. For the hacker the more the better so be careful.

It is also wise to not send passwords via email and if you do it is bes to use obfuscating techniques. For example if I was to send a password which is 12321 I would send it as:

1*2*3*2*1

or

1
2
3
2
1

You could also use PGP. Below is a more detailed form of what this is.

PGP (Pretty Good Privacy)

PGP is a data encryption and decryption software that provides Cryptographic privacy for data communication.

This software uses a serial combination of hashing, data compression, symmetric cryptography and public key cryptography. Each public key is bound to a user name and/or an e-mail address.

Hashing -

Hashing is a procedure that takes a block of data and returns a fixed-size bit string hash value. A accidental or intentional change to the data will change the hash value. The data encoded is usually known as the "message" and the hash value is usually known as the message digest.

Data Compression -

Data compression is the process of encoding information using fewer bits than an un encoded copy would use. This is done using specific encoding schemes. The sender and receiver both must know the data encoding scheme used.

You can get a free version of this software. To find out more go to

http://www.pgpi.org/products/pgp/versions/freeware/winxp/8.0/