



Beginning Computing: Safe and Comfortable?

*These instructions are aimed at IBM compatible Personal Computers (PC).
It is assumed that you can switch your computer on and launch an application.*

Safety Summary: If you do nothing else read this!

- ☒ Install Anti Virus software and keep it up-to-date
- ☒ Ensure your Operating System is kept up-to-date
- ☒ Ensure you have a Firewall running
- ☒ Back up your data regularly (you maybe very grateful one day)
- ☒ Scan for Spyware regularly
- ☒ Ensure your Browser is kept up-to-date
- ☒ Make your wireless network secure

1 Being Safe

Computer crime is becoming more prevalent as many users take few precautions to prevent criminals "breaking into" their machines to steal information. In the worst case this can result in identity theft and major losses of money and trust but even minor security lapses can make you the target of junk mail which will become irritating and may be offensive. There are a number of sensible precautions you can take to reduce the risk of such problems.

Anti Virus Software

Anti-virus software will give you some protect you from Viruses, Worms, Trojans and Diallers - if you install it and most importantly keep it up-to-date. Collectively these 'creatures' are known as Malware and Anti-Virus software is only one of the lines of defence against them.

If you have antivirus software you should be able to find it listed via the Start > Programs menu. If it is active you will see a small icon on your task bar at the bottom of the screen.

➤ **Obtaining antivirus software**

Some questions to ask before buying/downloading anti-virus software:-

- ⊕ Does it run on my Operating System (Windows, Linus etc)
- ⊕ Does it have automatic regular updates
- ⊕ Does it offer telephone support on a freefone or low cost UK number
- ⊕ Does it offer e-mail contact details for support.

NB. You can't expect the same level of support from free antivirus software that you should get from licensed versions.

➤ **Running antivirus software: On demand scanning**

When you install antivirus software you should first run a full scan of your machine which will check the memory (RAM) and hard disk, but the software will also scan CD-ROM drives and other storage devices connected to the computer. This type of scan can take quite a while and is best done with nothing else running.

➤ **Running antivirus software: Memory-resident scanning**

This should become active when you start up the computer and it monitors all your computing activity. This includes new files that you create, new software that you install, files downloaded from the Internet or transferred from CD-ROM or floppy disk. Think of it as a benevolent Big Brother, constantly on the alert for malware trying to attack the system.

➤ **Running antivirus software: Updates**

Antivirus software is reactive rather than proactive which means that it needs to be continually updated with the latest threats. Unless your AV software was free you will have to pay a regular licence fee. Even if you have your software set to 'automatically update', it will fail to obtain the updates if you have not paid the licence fee. With the current threat level, daily updates are not uncommon.

Operating System Updates

Many types of malware exploit "holes" in your computers operating system. Updating your system regularly helps block the "holes" as they are discovered. Whenever holes are found (by IT security people or groups, malware writers or the software developer) the operating system manufacturer will issue a fix for the particular problem. These fixes are referred to as patches. To ensure that your computer is safe you need to obtain patches regularly for the software that you use. You can do this by accessing the software company's website, for example Microsoft's Windows Update web page and this can be set to operate automatically on your computer

'Critical updates' normally consist of only one program, or a small group of programs, specific to a particular problem.

'Service packs' normally contain a lot of programs, covering many problems that have been found and corrected. These fixes are supplied as a group rather than individually. Some of these patches can be quite large, and take a long time to download. See <http://update.microsoft.com>

Firewalls

A firewall provides a barrier between your computer and the Internet ensuring all the traffic between the two acting as a 'paranoid bouncer'. It can block hackers (people trying to access your computer) and some types of malware (worms). To be effective you must also have antivirus software and not give permission for other computers to connect to yours without being sure that the other user is trustworthy.

- ⊕ Windows Firewall has a basic firewall built in (if you have kept your Operating system up-to-date) but you can replace it with a more sophisticated commercial firewall if you wish.
- ⊕ A commercial firewall to give you some extra protection and this may be bundled in with other security products.
- ⊕ Some broadband internet routers have a 'hardware firewall' which you can configure from your computer and though this is not always very simple.
- ⊕ Don't forget to change the routers password from its default setting (know by most hackers).

The basic version of the ZoneAlarm firewall is free for personal use. See <http://www.zonealarm.com>

Back ups

The most valuable part of your computer is the data on it, all those family photos, mp3 downloads..... Your hard drive could fail, your machine be stolen, a critical file accidentally deleted; the possibilities of disaster are almost endless.

- ⊕ Be organised about your data by keeping it in the same folder (eg My Documents) for easy back up. (NB My Documents can have multiple sub folders for organisational convenience)
- ⊕ You only need to back up your own files not the operating system or programs.

- ⊕ You can back up on lots of different types of media, CDs, DVDs or another hard drive. External hard drives which plug into a USB socket have become very cheap. You may wish to encrypt or password protect your backups.
- ⊕ You may consider leaving your back up with a friend or colleague if you are going to be away for any extended period (off-site back up)!
- ⊕ A number of companies offer online storage which you can used to back-up your data. Some offer this service for free but in the past a number have then subsequently want to charge you or have gone bankrupt.
See http://www.dmoz.org/Computers/Software/Internet/Site_Management/Backup/

The process of backing up can be as simple as using the copy software already built into your computer.

Downloads

Downloading is a method of obtaining information and most frequently software from the web using you internet connection. They are also a good way of getting some very unpleasant forms of Malware.

Some rules:-

- ⊕ Only use websites you trust.
- ⊕ Be very wary of any unsolicited invitation to download something.
- ⊕ Don't use Peer-to-Peer (P2P) networks which are riddled with viruses
- ⊕ Always have you antivirus software running
- ⊕ If you are not sure about the offering; search for it on the web to see what others say
- ⊕ Read the small print to ensure the software is compatible with your system
- ⊕ Read the small print again and make sure you are not agreeing something you want to avoid.
- ⊕ Before download or install any software back up you system.
- ⊕ If the software offered seems too good to be true, it almost certainly is!

Spyware

Spyware is another form of Malware which can report your use of your computer, inject adverts into your browsing, hijacks some of your software (most commonly your Browser) and in extreme forms capture personal information and send it to their creators for criminal purposes.

Adware is a form of Spyware that monitors your surfing and displays unwanted adverts on a computer.

To prevent Spyware entering your machine:-

- ⊕ Follow the downloading rule above carefully
- ⊕ Read the small print on licences to ensure that you aren't allowing Adware to be installed on your computer.
- ⊕ Use anti-spyware software

Anti-spyware programs operate like anti-virus programs. You can obtain free anti Spyware from:-

- ⊕ Spybot <http://www.safer-networking.org>
- ⊕ Lavasoft <http://www.lavasoft.com>

eMail and forums

email is possibly the most common way to acquire malware but there are also lots of other less serious irritations (such as spam) that could come your way. Some simple rules:-

- ⊕ Always save attachments before opening them to give your anti-virus software a chance to work
- ⊕ Delete all e-mails, unread, from people you don't know
- ⊕ Don't reply or attempt to unsubscribe to spam (It just confirms they have live email address)
- ⊕ Don't forward chain e-mail letters; they are never from legitimate organisations.
- ⊕ Don't forward warning about viruses etc, they are usually hoaxes
- ⊕ Never send sensitive information (bank details etc) by normal email

➤ **Phishing**

Typically you receive an email purporting to come from your bank or Building Society asking you to provide the security details of your account for some bogus reason. There may be a link which takes you to a website which is an exact facsimile of the normal website and on entering you details criminals are in the position to access and empty your account.

Financial institutions will never ask for this information by email; if in doubt phone to check.

Surfing the Web Safely

Like Operating Systems Browsers have 'holes' which can be exploited and updating your Browser regularly helps reduce the possibility of Malware intruding into your computer. This is usually done automatically by the software itself

➤ **Buying online**

- ⊕ Use companies which already have a good reputation.
- ⊕ Check they give actual addresses and phone numbers on their website.
- ⊕ Do they have clear privacy and returns policies?
- ⊕ Concerned? Search for them on the web and see what others say.
- ⊕ Concerned? Right click somewhere on a webpage and chose properties from the drop down list to see the actual URL which maybe very different from what you expected.
- ⊕ If giving critical information (eg credit card number) ensure you are on a secure website
The URL should have the letters 'https' in front of the web address; 's' standing for secure.
There should be a yellow padlock INSIDE the Browser border, not on the webpage.

➤ **Buying using an online auction (eg eBay)**

- ⊕ Read to rules to understand how the system works
- ⊕ Create a login name different from your email address
- ⊕ Use a strong password
- ⊕ Pick good sellers; look at their rating and transaction history.
- ⊕ Check the extra costs; packing, delivery costs, credit card surcharges etc
- ⊕ If it's a business, check they really exist
- ⊕ If the seller is outside the UK it maybe difficult to get things put right if they go wrong.

➤ **Using Social Websites**

Social networking site such as Facebook, Bebo, Twitter and MySpace etc allow people to build online networks of friends linked by shared interests. They do have risks of online bullying, stalking, loss of privacy and identity theft. Some tips to stay safe:-

- ⊕ Create a user name that doesn't include any personal details which enable you to be identified.
- ⊕ Create a separate email account to use on the site
- ⊕ Don't publish any personal information
- ⊕ Restrict access to your profile
- ⊕ Be careful who you let join your network.
- ⊕ Report bullying or harassment

Passwords

Many systems depend on passwords for security protection, but how good is your password?

- ⊕ Make it at least eight characters long; long passwords are harder to guess or break.
- ⊕ Don't use any proper names (company, pets, favourite teams etc)
- ⊕ Mix lower and upper case letters and some symbols
- ⊕ Use different passwords for different purposes, particularly for financial sites
- ⊕ Change it regularly
- ⊕ Don't tell anyone your password
- ⊕ Never send your password by email (as safe as a postcard)!

Using Wireless Based Systems

Many Broadband routers use wireless networks and although they only have a short range this may well extend well beyond the boundaries of your property making your network available to neighbours and passers by. This has a number of risks:-

- ⊕ **Freeloading:** Other users using your Internet connect for their own purposes slowing your connection and effectively accessing websites using your identity.
- ⊕ **Eavesdropping:** listening in to your communications gives the opportunity to capture passwords and any credit card numbers you transmit.
- ⊕ **Hacking:** using your wireless network to hack into your own computers in order to steal personal information.

➤ Securing your Wireless Network

You will need the manual, which came with your wireless router. This is frequently on the CD-ROM supplied with the router although you may have to download it from your ISP's website or even the manufactures website.

Unfortunately every router has a different procedure for carrying out the basic changes suggested below and you will have to rely on your manual for the details necessary.

When the wireless router was delivered it was set with the manufactures default settings (well know to Hackers) and it is these you must change to secure your network.

- ⊕ **Change the network name**
This is often called the SSID (Service Set Identifiers) and you should use something obscure (and long ,> 15 characters) as a new network name (not personal, street or pets names).
- ⊕ **Ensure encryption is enabled**
Encryption should be switched on and the type of encryption used will depend on the age of your router. Moving down in sophistication and level of security there are:-
 - WPA2
 - WPA-PSK (or WPA-Personal)
 - WEP-64 bit
 - WEP-128 bitSome encryption is certainly better than none. If a password or pass phrase is required make it long and non-obvious.
- ⊕ **Stop the network broadcasting its name**
Switch off the SSID broadcast. This is not possible with all routers.
- ⊕ **Change the access password**
Did you use the manufactures password to access the wireless routers management system? Again the password was probably the manufactures default and you should change it.

Additional Information

Get Safe online is an excellent Government sponsored website
The OU's **Safe Computing** website is run by the MCT faculty
DMOZ has lots of information available

<http://www.getsafeonline.org>

<http://safecomputing.open.ac.uk>

<http://www.dmoz.org/Computers/Security>

2 Being Comfortable

If you are going to use a computer a lot it's worth while spending some time ensuring that you have a comfortable working position to avoid any wrist, back and eye problems. This guide gives some ideas on how you can set up your computer working area and some guidance on good working practice.

If you are an Open University Student or Tutor more advice is available at the University website.

The key principle is to adjust the workstation to your needs, not the other way round. If you use a computer at your place of work your employer they will have a formal procedure for assessing your computer workstation which you should use.

➤ **Unpacking**

If you will be unpacking or moving equipment it's best to get help as some items can be very heavy and maybe awkward to manoeuvre.

➤ **Locating your Computer Workplace**

At home this will always be a compromise between:-

- ⊕ Easy physical access for you
- ⊕ A good working environment: not subjected to interruption and noise
- ⊕ Glare free lighting: avoiding reflections on the screen from windows or lights
(This may require temporary use of curtains or blinds)
- ⊕ Easy access to services: power and telephone points
(Avoiding trailing cables and overloading power sockets)

➤ **Table/workstation**

This need not be a specialist computer workstation as long as the table/chair combination enables you to fulfil the basic requirements suggested below.

- ⊕ The table should be large enough for your screen, keyboard, mouse and any documents you are working on (your printer can be a little remote providing the cable is long enough).
- ⊕ The table surface should ideally be a light coloured and non reflective
- ⊕ There should be enough legroom to enable you to sit comfortably, move your legs freely and reach the keyboard without stretching

➤ **Positioning**

- ⊕ Place the screen in the centre of the workstation (NB beware some screens are very heavy)
- ⊕ Place the keyboard directly in front of the screen but leave some space (10cm/4 ins) in front of the keyboard so that you can rest your wrists.
- ⊕ Place the mouse to the right of the keyboard on the same surface (if you are right handed).

➤ **Chair**

If you are going to spend an appreciable time at your computer it's worth investing in a good office style chair. It must be stable (5 branch base) and have the following adjustments: seat height, seat tilt and backrest height and tilt. Armrests are not essential and if you get them ensure they can be removed easily later if necessary. Good breathable padding will add to your comfort.

➤ **Adjusting the Chair**

- ⊕ Adjust the seat tilt until you feel comfortable (level or tilting slightly forward is usual)
- ⊕ Ensure there is no excessive pressure on the backs of your legs.
- ⊕ Adjust the seat height so that you can rest your fingers on the home keys of the keyboard with your fore arms straight without your shoulder being hunched (Your upper arms should be vertical).
- ⊕ Adjust the backrest so it supports the small of your back
- ⊕ Your feet should be flat on the floor and you should be able to move your legs freely.
(If your feet don't touch the floor you should consider getting a footrest.)

➤ **Screen**

- ⊕ Adjust the height of the screen so that the top is at, or slightly below your eyeline
- ⊕ Move the screen back and forth so that it is at arms length (40-70cm) when you are sitting normally in your chair with your fingers on the keyboard.
- ⊕ Tilt the screen so that it is at right angles to your line of sight

Working Well

➤ **Screen**

- ⊕ Adjust brightness and contrast controls to suit your lighting conditions
- ⊕ Ensure that the image on the screen is sharply focused with no flicker
- ⊕ Adjust the text size to suit your own needs
- ⊕ Ensure you have good contrast between text and screen background
- ⊕ Keep the screen clean but be sure to follow the manufacturers instructions (Some screens can be easily damaged).

➤ **Work Organisation**

- ⊕ Take frequent breaks to do other things; short breaks (5mins every 60mins) are better than longer less frequent breaks (Use a kitchen timer as a reminder).
- ⊕ Look away from the screen into the distance about every 5 mins to give your eyes a chance to relax.
- ⊕ Use a document holder if you are going to do lots of copy typing (Position it at the same level, height and distance as the screen)
- ⊕ Don't have too many windows open at a time on your screen.

➤ **Posture**

- ⊕ Change your sitting position now and again
- ⊕ Don't over stretch your fingers when using the keyboard
- ⊕ Keep your wrists straight and level
- ⊕ Type lightly to reduce the impact on your wrists
- ⊕ Use a relaxed grip on the mouse, especially when not actually using it
- ⊕ Move your arm rather than your wrist

➤ **Eyeware**

A screen can be at intermediate distance for some spectacle wearers and a few may require different glasses. Vari/bi/trifocals can be problematic if you have to titling your head to peer through the lens and this can cause neck problems. If you work for a commercial organisation they should be able to provided specialist eyeware.

➤ **Being safe and environmentally friendly**

- ⊕ Ensure none of the ventilation slots on your computer, screen etc are even partly blocked
- ⊕ Don't hide main cable under the carpet where they can be damage or may overheat.
- ⊕ Power down and switch off you computer at the end of the day
- ⊕ Unplug your mains and telephone lead if there is a local thunderstorm. (Lightening strikes on overhead phone lines can do a lot of damage).

➤ **Working with others**

Most of us have to share our computer with other members of the family who may be very different in size and shape and the computer workstation must be capable of adjustment to their needs. Principally this means your chair should be adjustable and you may have to have some method of changing the height of the monitor.

Using a Laptop

All the advice above holds true but...

- ⊕ The rigid connection between screen and keyboard give poor compromise between viewing and typing requirements
Use additional external keyboard and/or monitor if possible
Or get docking station
- ⊕ Always use firm surface to type on
- ⊕ Trackerpads are usually in centre of the laptop 'keyboard' resulting in a bent wrists (which can cause problems)
Use an additional external mouse if possible
- ⊕ Text legibility can be poor if the user changes the suggested text sized (due to flat screen construction)
- ⊕ Keep the weight you carry down
Don't carry unnecessary peripherals or get wheeled bag
- ⊕ NB some laptops can get quite hot in normal operation, which can be a surprise if you place them on your lap!

More Information

On setting up your workstation

HSE (Health and Safety Executive) website
for advice on

<http://www.hse.gov.uk>

- ⊕ Manual Handling (lifting etc)
- ⊕ Working with VDUs
- ⊕ Risk Assessment

IBM's Healthy computing site.

<http://www.pc.ibm.com/ww/healthycomputing>

HP's Safety & Comfort Guide (with downloadable guide)

<http://www.hp.com/ergo>

Resources for Open University Students & Staff

On using your computer

<http://www.open.ac.uk/computingguide/start.html>

PC4Study; covers Communicating, Writing and Searching

<http://www.open.ac.uk/pc4study/index.php>

Tips and advice for using the web effectively

<http://www.open.ac.uk/webguide>

Safari: the OU Library's information training course (free)

<http://www.open.ac.uk/safari>

Soft skills eg effective study, managing stress etc

<http://www.open.ac.uk/skillsforstudy>