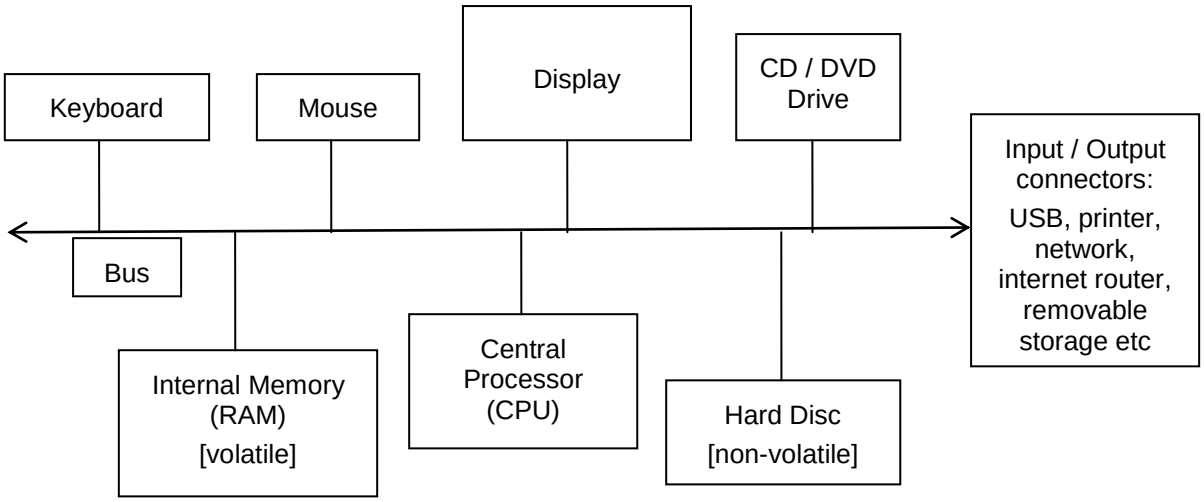
RADLETT & DISTRICT

U3A
THE UNIVERSITY OF THE THIRD AGE

Computer Group Notes

Security and Backing Up

Block Diagram of a computer



Security software:

Choosing the best antivirus software Antivirus software top tips

If a web address starts with **https**, the site is secure.

Dos and don’ts for security software

Do...

• Keep your operating system’s built in firewall and anti-spyware tools switched on until your new software is installed.
• Make sure you’re only running one antivirus program
• Scan your computer regularly for malware
• Turn on automatic updates for your security software and operating system
• Check your junk email folder in case legitimate messages have ended up here
• Beware spoof security alerts
• Make sure your wireless network is secured

Don’t...

• Install more than one antivirus program
• Download programs from sources you don’t trust 100%
• Open suspicious email attachments or web links

Security software: Choosing the best antivirus software Types of antivirus software

Spyware is installed on your computer without your knowledge and can disrupt your system with unsolicited pop-up windows and even literally ‘spy’ on your computer activity, secretly sending your private information to criminals.

Good anti-spyware software is designed to both remove any spyware it detects on your computer and prevent any further spyware from becoming installed.

It should work in two main ways, providing real-time protection from spyware infection, whilst also allowing you to perform regular system scans, preferably as part of an ongoing automatic security schedule.

The line between anti-spyware and anti-virus software has blurred over the years but it's worth noting that, while many anti-virus products now also include spyware protection, most dedicated anti-spyware programs don't usually protect against viruses.

Do I need it?

Absolutely – all computers need to be protected against spyware. Windows 7 and Vista PCs come with a built-in anti-spyware program called Windows Defender, which is also available as a free download for XP users. Most internet security suites also include anti-spyware features and there are also several free alternatives available for PCs, including Spybot Search & Destroy and PC Tools Spyware Doctor. Mac users should consider an all-in-one anti-virus and anti-spyware tool, such as MacScan.

Antivirus programs

Most antivirus programs would be better described as 'anti-malware', since they are often designed to protect against worms, Trojans and most other types of malicious software as well as viruses.

Some even protect against spyware, but it doesn't hurt to have a separate anti-spyware program installed, too.

Most anti-virus programs identify malware by comparing signatures to a built-in database of known malicious software types. This database needs to be kept up to date in order to ensure protection, which is why it's vital to download updates as soon as they're available. Some anti-virus programs also use techniques called 'heuristic detection' and 'sandboxing' to help identify new types of malware as they appear.

Do I need it?

Anti-virus software is essential. Neither Apple Macs nor Windows-based PCs come with any kind of anti-virus software and it's vital to install some yourself. Anti-virus programs can be purchased on their own or as part of an internet security suite. There are also many good free anti-virus programs available, such as Microsoft Security Essentials.

Browser security

A web browser is the program used to view pages on the internet, such as Internet Explorer, Safari, Firefox, Opera and Google Chrome.

It's possible for malware, hackers and other cyber criminals to exploit weaknesses in web browsers. As such, you need to make sure that you're using the very latest version of your chosen browser and that you keep it up to date.

The web browsers mentioned above also include a number of other security features, such as pop-up blockers and phishing detectors, which can warn you if a website appears to be a fraud. These tools should be turned on by default, but you can usually check by looking under the relevant section of the Tools, Options or Settings menu.

Do I need it?

Everyone needs a web browser to surf the web. As long as you're not using an old version, then you shouldn't have to worry – all the latest versions of popular browsers include phishing detectors and other useful built-in security features. Your browser needs to be kept up to date in order to stay safe but, again, the latest versions have this covered thanks to their auto-updating features.

Firewall

Your firewall is your first line of defence against hackers and other types of unauthorised access to your PC from over a network or the internet.

A firewall works in the background all the time monitoring traffic to (and, in some cases, from) your computer. The firewall blocks certain ports and only allow specific programs and services to communicate with your PC.

Do I need it?

A firewall is essential. Some routers have built-in firewalls, but you need to have one running on each of your home computers as well in order to be safe. Both Windows and Mac OS X come with built-in firewall software but, as mentioned here, the default settings they operate on don't necessarily provide the best protection.

It may be worth considering using an alternative – one that can monitor both outgoing and incoming traffic. Virtually all commercial security suites contain a powerful bi-directional firewall but there are several very good free equivalents that can be used instead, such as Zonealarm.

Parental controls

These are programs that allow you to limit and, in some cases, monitor specific people's computer use. Usually this means parents (or grandparents) restricting the number of hours their children can use the PC, blocking the use of

certain programs (including blocking games by their age rating) and limiting internet access to known safe sites in order to prevent children from being exposed to anything unsuitable online.

Windows 7 and Vista PCs and Apple Mac computers both come with some basic parental control features and there are other paid-for (such as Net Nanny) and free (such as K9 Web Protection) alternatives.

Do I need it?

If you have children or grandchildren, or if for any reason you need to limit computer use or restrict access to certain files, programs or websites, then parental controls are extremely useful, since you can't always be there to supervise.

Phishing protection

Phishing scams usually take the shape of a two-pronged attack that starts with a fake email posing as if it is from a genuine source, such as your bank, that then points you towards an equally fake website in order to con you into parting with vital private information, such as your credit card number.

Protecting from them takes a similarly two-pronged effort, with anti-spam software (see below) filtering out unsolicited emails and web browser security features (see above) protecting against known fraudulent sites.

Do I need it?

We thoroughly recommend using a spam filter; these can significantly reduce your chances of being exposed to a fraud. And it's vital to use the latest web browsers, which all have anti-phishing features switched on by default.

Spam filter

Also known as anti-spam software, these utilities act like a sieve, letting through legitimate email messages but blocking unwanted or unsolicited mail from reaching your inbox.

Ask your internet service provider about spam filtering – you may find that your ISP is already employing spam protection on its servers. It's still a good idea to have your own spam protection on board too.

See our advanced email tips for help on managing spam

Some email programs, such as Apple Mail, Microsoft Outlook 2007 and the free email program Thunderbird, come with built-in spam filters. Most of the big security suites come with an anti-spam element too.

Do I need it?

Spam is a big nuisance, but it can also be the method of transmission for some far more worrying phenomena; phishing scams and malware attachments are also common. As such, anti-spam protection is vital tool in order to minimise your chances of being exposed, compromised or infected.

From Wikipedia, the free encyclopedia

Mailwasher

Mailwasher is an e-mail filtering software for Windows, Unix, and Macintosh systems that can detect and delete spam from a user's e-mail when it is on the mail server, before being downloaded to the user's computer.

Mailwasher was developed by the New Zealand based company Firetrust. It uses a combination of user defined filters, spam databases and Bayesian filtering. The filter works on a small portion of each email, and then allows unwanted emails to be directly deleted from the user's POP3 inbox, without downloading them to the e-mail client on the user's computer. This approach is intended to prevent the downloading of spam and other messages infected with malware.

There are two versions of the program. The free version can access only a single mail account and does not contain the Bayesian learning filter. The Pro version can access multiple accounts and has additional features.