University of BRISTOL

IT Services

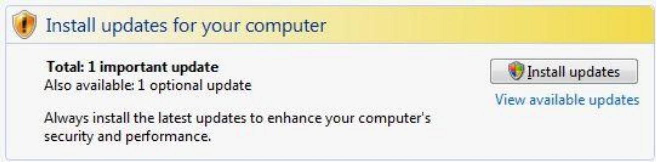
Windows laptop security advice

Advice for laptop owners on how to keep your computer secure and virus free.

Your computer needs regular attention to keep it secure from viruses, spyware or hijacking by criminals and it is your responsibility to do this. Even if you have asked the IT Service Desk or the Student Laptop and Mobile Clinic to help remove a virus from your laptop then you should still follow this advice to ensure continued security.

Microsoft Updates

Install all Microsoft Updates. Microsoft release frequent patches for security vulnerabilities in their software and it is vital that these are installed when released

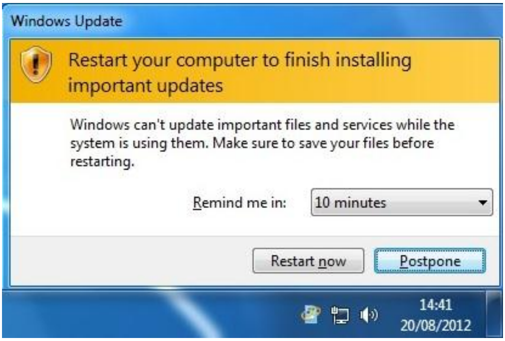


Install updates for your computer

Total: 1 important update
Also available: 1 optional update

Always install the latest updates to enhance your computer's security and performance.

This is normally an automatic process, though you may see the following window asking you to restart your computer to complete installations.



Windows Update

Restart your computer to finish installing important updates

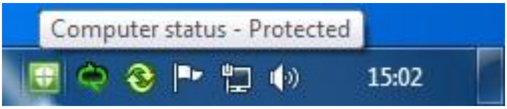
Windows can't update important files and services while the system is using them. Make sure to save your files before restarting.

Remind me in: 10 minutes

You can also start Windows Update by clicking on the **Start** button, then click **All Programs**, and then click **Windows Update**, (from where you can also configure your system to auto update) or by browsing to `update.microsoft.com` via Microsoft Internet Explorer.

Virus Checker

Ensure that your virus checker is active and up to date.

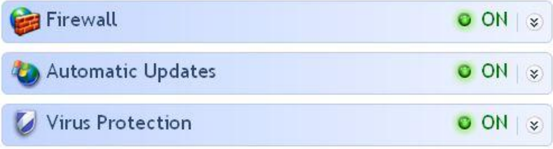


Computer status - Protected

If you purchased a licence for a virus checker then ensure that it has not expired, otherwise use a free virus checker like Microsoft Security Essentials, (only install one virus checker at a time, otherwise they won't work). It should be set to frequently automatically update the virus definitions.

Firewall

Ensure that your computer's firewall is active. Windows XP, Vista and 7 have a built-in firewall which is adequate. Click on "Start", "Control Panel", "System & Security", ("Security Centre" in Windows Vista) and ensure that it is switched on, (Vista shown below).



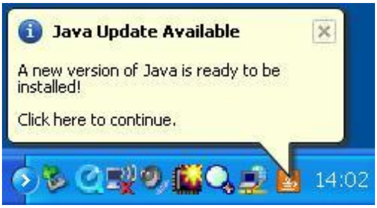
Firewall ● ON

Automatic Updates ● ON

Virus Protection ● ON

Update software

Keep all of your software up to date, this is very important and often overlooked. Adobe Flash, Java, Adobe Reader, Quicktime, Real Player, Skype and most especially any other software that connects to the internet, (such as e-mail clients and web browsers) need to be kept up to date. Go to their websites, download the latest version and follow their instructions to install it. Or scan your computer for vulnerabilities using Secunia PSI, free to download from: www.secunia.com/vulnerability_scanning/personal



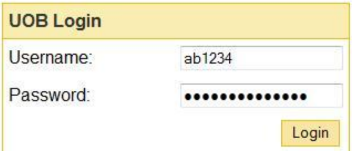
Java Update Available

A new version of Java is ready to be installed!

Click here to continue.

Change passwords

Change your passwords from a trusted computer, especially if your computer was infected with a virus which steals passwords. Use strong passwords that cannot be easily guessed, including upper case and lower case letters, numbers and other characters. Use different passwords for all accounts, (bank, Facebook, etc.) most especially a separate one for your University account.



UOB Login

Username: ab1234

Password: ••••••••••••••

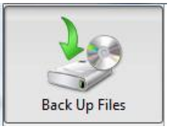
Admin rights

Do not go online whilst logged in to your computer with administrator rights, especially if you are using Windows XP. Logging in with administrator rights allows you to install software and patches but also allows malware to install and run itself without your knowledge. You should add a new user account without admin rights and use that account for normal use.

Malware removal

Run a malware or spyware removal tool separately from your system's virus checker to double-check for viruses or other malware. Software such as MalwareBytes or Spybot are useful for removing spyware. Follow the anti-spyware link on the Protect your PC section of our Information Security website for more information on these. Once you've installed them remember to update and run them frequently, especially after a virus infection.

Backup data



Backup your data regularly. Your operating system and software can be reinstalled but if you lose your data then it may not be replaceable. A good method is to backup regularly to an external USB hard-drive, which are relatively cheap to purchase.

Surf safely

Your bank will not ask you to send your username and password by insecure e-mail to them, neither will someone really offer you $30million if you send them your bank details and the University will not ask you to confirm your password via e-mail. A flashing popup window claiming that you are infected with viruses and need to download new software is called Scareware and is an advert, rely on your own virus checker. Be very suspicious of such requests, offers and popups.

Reinstall Windows

The only way to ensure that your computer is free of virus infection is to wipe it and reinstall Windows from scratch. You may have used software such as MalwareBytes to clean the computer but that is no guarantee that the viruses have been completely removed. Wiping and reinstalling will wipe any viruses still hiding on your hard disk but be warned that it is a lengthy process involving backing up data, wiping the hard-drive, reinstalling Windows, reinstalling programs and updates.

You do not have to do this process, it is not the next step after the previous steps in this leaflet but it is important that you know about it. If you decide to take this route then you may wish to seek advice from someone technically literate. This is not a service that the University provides; neither the IT Service Desk nor the Student Laptop and Mobile Clinic can reinstall Windows for you.

Refer to your computer manufacturer's website for advice on how to reinstall, whether using a restore CD that came with the computer, a genuine Windows CD or a reset from a partition on the hard-drive. This varies per make of computer, the manufacturer's website will have a support section that can advise on this. More information on this process can be found at:
http://www.bristol.ac.uk/it-services/advice/homeusers/software/restorewindows.html

Information Security website

More information on all of the points in this leaflet can be found on our Information Security website at www.bristol.ac.uk/infosec and we advise that you read that website and keep yourself abreast of any changes to it in the future.

For further advice

Contact the IT Service Desk

- Email: service-desk@bristol.ac.uk
- Phone: (0117) 928 7870
  internal 87870.
  Mon-Fri 8:00am - 5:15pm
- In Person: Computer Centre first floor.
  Mon-Fri 9:00am - 5:00pm

Visit the Student Laptop and Mobile Clinic

- www.bristol.ac.uk/laptopclinic