

<http://www.darc-tech.org.uk/>

If you have any questions about anything contained within the document, feel free to ask me. I'm afraid it does focus mainly on Windows-based software, since the user base for Windows PCs is much greater than any other OS.

Here is information and links for software that will help to protect computer users. I've included a list of essential strategies, complete with a number of useful links.

The main site I recommended for downloading all manner of software is <http://downloads.cnet.co.uk/> - this is the UK site; there is also <http://download.cnet.com/windows/> - this is the US site. Both sites have every kind of software, as well as for Macs, mobiles and so on. Their downloads are certified virus-free, and very reliable.

1) Install and update antivirus software. It needs to be updated regularly, not every month or even every week. Most antivirus software will try to update itself every day - let it! Free antivirus packages can be downloaded from:

<http://free.avg.com/gb-en/download-avg-anti-virus-free> - make sure you pick the free edition!

<http://www.avast.com/en-gb/free-antivirus-download> - I use this product and find it very reliable and secure. Again, choose the free version.

<http://www.bitdefender.com/PRODUCT-14-en--BitDefender-Free-Edition.html> - another well regarded free package

<http://www.pctools.com/free-antivirus/> - and another company whose products I really rate very highly!

http://www.lavasoft.com/products/ad_aware_free.php - and one more, which combines antivirus with antispyware and other security measures, all for free!

2) Install and update antispyware software. Again, this needs to be done daily, so that you don't leave your machine unprotected against the latest threats. This can be included with antivirus software, such as with Ad-Aware.

http://www.lavasoft.com/products/ad_aware_free.php - comprehensive free protection.

<http://www.safer-networking.org/en/spybotsd/index.html> - Spybot Search & Destroy comes highly recommended, and works away silently protecting you from dodgy sites.

<http://software.techrepublic.com.com/search.aspx?q=Rocket+division+AntiSpyware+2010+2.7> - and one more. To be honest, the first two are pretty much universally recommended, unless you feel like paying for a commercial product. I would recommend installing both Ad-Aware and Spybot Search & Destroy.

3) Use a firewall at all times. Firewalls hide your computer from other users of the Internet. If they don't know you're there, they can't try to attack you. If you have broadband, you probably have a router which may have a firewall included. Even if it does, you can still install a software firewall as well. If you want to TEST the security of your system, go to <http://www.grc.com/intro.htm> and follow the links until you get to the ShieldsUP!! tests - this will check to see whether your machine is protected or not. If it isn't, it will alert you to the fact, so that you can remedy the situation. In the event that you are unsure how to secure your system, please contact me, and I will do my best to guide you through what needs to be done. As for free firewalls:

<http://www.zonealarm.com/security/en-gb/anti-virus-spyware-free-download.htm> - the ZoneAlarm Free Firewall is very highly regarded, and protects you more than Windows' own built-in firewall (*which you*

should really only use until you get something else, and then turn it off! - You must not run two software firewalls at the same time...).

<http://www.pctools.com/firewall/> - this is the firewall I use, and it runs more easily on netbook computers than ZoneAlarm: highly recommended, and very effective.

<http://www.comodo.com/home/internet-security/firewall.php> - another very popular and effective free firewall.

http://www.privacyware.com/personal_firewall.html - and one more!

All of these 3 pieces of software should be running on your computer, and should be updated regularly - firewalls don't usually need to be updated as often as the antivirus and antispyware.

4) Keep your Operating System updated. This means Windows or MacOS X or whatever you use to run your computer. Microsoft release regular updates at least once every month - if problems are found, they will release additional updates. These updates are designed to block problems that have been found. If your machine isn't updated, you remain more at risk. It may seem annoying to have to wait whilst the updates are downloaded and installed, but it is essential to keep your machine secure and also more reliable.

5) Be careful about the things you download. Never open websites or attachments in email that has come from someone you don't know. Banks will NEVER ask for any security information in an email, and will NEVER provide a link for you to click on in order to get to their website, so if you get an email asking you to click a link, it will almost certainly be a phishing email trying to trap you into giving away personal information. If you know the address you want, type it in yourself. If you don't know it, use one of the major search engines, such as Yahoo or Google, and find it that way. Once you find it, save it as one of your Favourites or Bookmarks, so that you can go back to it easily in future. For example, I access my online banking using a favourite every time. If your bank offers additional security software or features, it is worthwhile using them. Remember that secure websites can be identified by https at the start of the website and often a padlock icon (either at the top or the bottom of the page). The latest versions of web browser software will check that the website you're trying to connect to is reliable. This can slow things down ever so slightly, but is a small price to pay for the additional security.

6) Turn off your computer! No one can attack it when it's turned off! It's tempting to leave broadband connections on 24/7, and to leave the computer connected to the broadband connection as well. This could give someone more time to try to compromise your system. It is more of a hassle to have to turn everything on before you can check your emails or read the latest comments on your Facebook page - but turning the computer off also ensures that the software loads freshly each time you turn it on, and obviously will save electricity when everything is turned off! Sacrifice a little convenience for the sake of the security!

Obviously, my approach within this document is a little simplified, bearing in mind that target audiences are not usually computer experts. I do realise that I have made some statements that could be debated by some more knowledgeable people. The contents were never intended to be encyclopaedic in scope, so please don't take me to task over some of the simpler assumptions I have made! Thanks!

Bimal Jangra, Chairman - DARC Technology Club, PC Bits Columnist - Archive Magazine, Microsoft Certified Professional

Email: chair@dar-tech.org.uk