

Security threats posed by memory stick usage – Part 2



Use of USB memory sticks as discussed in the previous article, can potentially pose a threat to your computers or network.

Often by default they behave as 'plug and play' devices. You plug in your memory stick to your computer, it is automatically recognised and the drive and its contents displayed. Contents may even Autorun or AutoPlay.

Not only can you then deliberately or unwittingly transfer viruses, spyware and other malware from the memory stick to a PC / network (or vice versa), but there is also the opportunity for someone to easily export organisational data which may be confidential. This is especially a concern if you have PCs accessed by clients or the public.

To safeguard your PCs, laptops and networks there are a number of options you can deploy which act either locally on your machine or via your server / network environment.

How to disable the Autorun functionality in Windows

Windows AutoPlay – one of the Autorun options – means that Windows begins reading from a drive as soon as you insert media into it. For example the setup file of programs usually starts immediately without you being asked whether you want it to. Starting with Windows XP Service Pack 2, AutoPlay is enabled for removable drives including some USB mass storage devices.

Memory sticks and other removable media have become a very common method for spreading computer viruses and trojan horse malware, so you should seriously consider disabling the Autorun / AutoPlay option and especially if you have PCs used regularly by volunteers / clients / and members of the public.

This can be done either for a stand alone PC / laptop or by setting group policies on a server. For example if you only need to set this for Guest users who may for example be learners who use your training suite – AutoPlay can be disabled for their logins only.

Full instructions are given at <http://support.microsoft.com/kb/967715/> - please note the article mentions that you first need to make sure you have downloaded specific security updates.

In addition to disabling AutoPlay – you may even want to be able to prevent users from connecting to a USB storage device at all. Instructions for this can found at <http://support.microsoft.com/kb/823732/> and could be relevant to your organisation if you have sensitive data on the system and you wanted to safeguard against staff / volunteers / clients copying it and taking it off site.

Scanning Memory sticks for Viruses

Most branded antivirus software have on demand scan enabled; so that any removable media is automatically scanned when connected to the PC. However, you can also manually scan the memory stick by right clicking on the removable icon and selecting the scan for viruses option.

Usage Policies

As mentioned in the previous guidance, it is recommended to incorporate USB memory stick use in the organisation's Internet and computer usage policy by including best practice to reduce the risk from memory threats including:

- Use different memory sticks for work and personal use
- Do not use work memory sticks in Internet cafes or public access computers
- Do not give your memory stick to your friends and family to use as they could use it on infected computers