

Memory sticks and security



This brief guide covers the following topics:

1. Assessing the risk
2. Raising awareness with staff / volunteers
3. Purchasing a memory stick with built in encryption
4. Using encryption software with an existing memory stick
5. Other security threats posed by memory stick usage

1. Assessing the risk

Firstly it is useful to consider which is the more likely scenario:

- You accidentally lose your memory stick?
- Someone deliberately steals your memory stick in order to gain access to the data stored on it?

This leads us nicely into the second question...

What information are you carrying around on your memory stick?

- Is it personal data about clients which is highly sensitive?
- Or does it hold no real interest to anyone who happened upon it?

2. Raising awareness with staff / volunteers

If staff are given memory sticks so they can carry documents from the work place to home or outreach locations, first ensure that you have discussed the risks above. A good time to do this with new staff is during their organisational ICT induction.

As well as covering what data is sensible to carry around from place to place, it is also worth pointing out that best practice dictates that you regularly back up / synchronise memory stick data.

In this way – even if loss or theft occurs – you won't need to waste precious time redoing the work. You could use for example Microsoft's SyncToy www.microsoft.com/downloads/details.aspx?FamilyID=c26efa36-98e0-4ee9-a7c5-98d0592d8c52&DisplayLang=en to easily synchronise between your work PC, memory stick and laptop / home PC

3. Purchasing a memory stick with built in encryption

If security is recognised to be a high priority for your organisation or specific workers, you could make it a policy to buy memory sticks which have built in encryption – look out for use of the Advanced Encryption Standard (AES) preferably at AES 256.

To access the contents of the memory stick you first have to set a password and then enter this each time you use the stick. Some have a lockdown facility so for example if the password is guessed wrongly 6 times – the drive is permanently locked down.

Prices will be slightly higher for a secure memory stick. To give you an idea - Kingston's entry level 4 GB memory stick is around £5 whereas their Data Traveler 410 and Data Traveler Locker are around £12 - £15.

4. Using encryption software with an existing memory stick

Use of third party software like the open source TrueCrypt www.truecrypt.org will allow you to encrypt an existing 'insecure' memory stick.

You would first need to download TrueCrypt and install it on all the PCs / laptops you regularly use and then select whether you want to encrypt the whole memory stick drive or just a specific folder. A Beginners Tutorial to guide you through the process is available at www.truecrypt.org/docs.

Please be aware that you would need to take existing data off the memory stick before encrypting it and then transfer the files back again, otherwise they would be wiped during the encryption process!

Alternatives include Cryptainer www.cypherix.com/cryptainerle or FreeOTFE www.freeotfe.org – both of which offer 'portable' options where you can carry the program on the memory stick giving you greater flexibility over its use, though possibly as a result weakening its security.

5. Other security threats posed by memory stick usage

Use of USB memory sticks 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.

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.

A factsheet on this topic is currently being developed and will be available in Sept 2009.