

Play it safe

IN ASSOCIATION WITH



David Paine explains how you can protect yourself when you use your laptop away from the office

Beware the “evil twin”

If you use WiFi “hotspots” at airports and cafés, then read on... Do you know who owns the hotspot you are connecting to? Increasingly, hackers are easily creating rogue WiFi connections simply using a special USB thumb drive that acts as an access point. The access point can be named to look like the legitimate WiFi hotspot (hence its nickname: “Evil Twin”) and because the perpetrator’s laptop can be hidden in a bag close to where you are working, their network may have the stronger signal, which draws people to it. Once you’ve logged-on to the evil twin, all it takes is some basic programming for them to capture your credit card details when you log on, steal other personal information from your computer and redirect you to bogus sites they have set up.



Here are five steps to help protect you:

- 1 Make sure the access point is legitimate and don’t set your wireless card to connect automatically to any available network.
- 2 Encrypt and password-protect sensitive data.
- 3 Use a virtual private network (VPN) or a secure Citrix Solution. While this will protect your company data once you’ve logged on, it will not protect the credit card details you may use to log-on. Consider using only one credit card for online transactions.
- 4 Use an updated personal firewall and ensure that file sharing is switched off.
- 5 Be aware of your environment, especially in crowded places.

Protect yourself from laptop theft

Recent figures from UK police forces show that nearly 100 laptops a day are reported stolen – and you can be sure that more will go unreported. Replacing a laptop is not expensive, but what price would you put on the data contained? When considering the risk of losing a laptop, there are two main data considerations: retaining use of the data stored, and protecting the data taken from malicious sale or use.

Here are five steps to help protect you:

- 1 Employ a data encryption system, so the stolen data is useless.
- 2 Use strong but memorable passwords and never use the “remember this password” feature of Windows.
- 3 Use a storage device that enables quick daily back-up of all essential data.
- 4 Regularly audit your laptop to minimise the amount of sensitive data stored.
- 5 Try to keep your laptop in a less obvious place, such as a briefcase, rather than a laptop bag.

DAVID PAINE is technical services manager for Castle Computer Services. For help and advice on remote working email info@castle-cs.com, call us on 0845 230 1314 or visit www.castle-cs.com