

Laptop Security

Laptops are very common in the workplace and the home. They are easy to steal and more importantly it is easy for you to lose confidential data. Below are a number of tips to help you secure your laptops. If you want help with any of these, call Virtual Riders. Whilst no measure can guarantee the security of your machine and its data, incorporating (some of if not all of) these points into your staff policies on laptop use will help you meet your data protection obligations and may help for insurance purposes.

1 Basics

- a. Choose a secure operating system and lock it down
- b. Enable a strong BIOS password
- c. Asset Tag or Engrave the laptop
- d. Register the laptop with the manufacturer
- e. Place a hidden ownership label under the battery or under the memory access panel.

2 Physical

- a. Get a cable lock and use it
- b. Use a docking station
- c. Lock up your cards, USB devices/drives etc.
- d. Use a personal firewall on your laptop
- e. Use tracking software to have your laptop call home (if you are well off!)

3 Protect Your Data on the Laptop

- a. Use the NTFS file system
- b. Disable the Guest Account
- c. Rename the Administrator Account
- d. Consider creating a dummy Administrator account
- e. Prevent the last logged-in user name from being displayed
- f. Disable the Infrared Port and Bluetooth on your laptop
- g. Turn off wi-fi if you are not using it
- h. Backup your data before you leave/finish work
- i. Make a physical external copy of your work (to a CD/flash drive etc) but make sure it is secure/encrypted.

4 Guidelines for preventing theft

- a. Assume it is always vulnerable to theft
- b. Use a low key carrying case which doesn't look like a laptop bag
- c. Never put your computer bag down/out of sight when undertaking a task which requires your full attention (registering, paying a bill etc)
- d. Always put your laptop in the (lockable boot of a car
- e. Hide/secure your laptop if leaving it in a hotel room