



This advice has been produced to help small businesses protect themselves from the most common cyber attacks. The 5 topics covered are easy to understand and cost little to implement. Read our quick tips below, or find out more at [www.ncsc.gov.uk/smallbusiness](http://www.ncsc.gov.uk/smallbusiness).

## Backing up your data

Take **regular** backups of your important data, and **test** they can be restored. This will reduce the inconvenience of any data loss from theft, fire, other physical damage, or ransomware.



**Identify what needs to be backed up.** Normally this will comprise documents, photos, emails, contacts, and calendars, kept in a few common folders. Make backing up part of your everyday business.



**Ensure the device containing your backup is *not* permanently connected** to the device holding the original copy, neither physically nor over a local network.



**Consider backing up to the cloud.** This means your data is stored in a separate location (away from your offices/devices), and you'll also be able to access it quickly, from anywhere.

## Keeping your smartphones (and tablets) safe

Smartphones and tablets (which are used outside the safety of the office and home) need even more protection than 'desktop' equipment.



**Switch on PIN/password protection/fingerprint recognition** for mobile devices.



Configure devices so that when lost or stolen they can be **tracked, remotely wiped or remotely locked**.



Keep your devices (and all installed apps) **up to date**, using the '**automatically update**' option if available.



When sending sensitive data, don't connect to public Wi-Fi hotspots - **use 3G or 4G connections** (including tethering and wireless dongles) or **use VPNs**.



Replace devices that are no longer supported by manufacturers with up-to-date alternatives.

## Preventing malware damage

You can protect your organisation from the damage caused by 'malware' (malicious software, including viruses) by adopting some simple and low-cost techniques.



**Use antivirus software** on all computers and laptops. **Only install approved software** on tablets and smartphones, and prevent users from downloading third party apps from unknown sources.



**Patch all software and firmware** by promptly applying the latest software updates provided by manufacturers and vendors. Use the '**automatically update**' option where available.



**Control access to removable media** such as SD cards and USB sticks. Consider disabling ports, or limiting access to sanctioned media. Encourage staff to transfer files via email or cloud storage instead.



**Switch on your firewall** (included with most operating systems) to create a buffer zone between your network and the Internet.

## Using passwords to protect your data

**Passwords** - when implemented correctly - are a free, easy and effective way to prevent unauthorised people from accessing your devices and data.



Make sure all laptops, Macs and PCs **use encryption products** that require a password to boot. Switch on **password/PIN protection** or **fingerprint recognition** for mobile devices.



**Use two factor authentication (2FA)** for important websites like banking and email, if you're given the option.



**Avoid using predictable passwords** (such as family and pet names). Avoid the most common passwords that criminals can guess (like *passw0rd*).



Do not enforce regular password changes; they only need to be changed when you suspect a compromise.



**Change** the manufacturers' default passwords that devices are issued with, before they are distributed to staff.



**Provide secure storage** so staff can write down passwords and keep them safe (but not with the device). Ensure staff can reset their own passwords, easily.



**Consider using a password manager.** If you do use one, make sure that the '**master**' password (that provides access to all your other passwords) is a strong one.

