Organisations can carry out the following actions in accordance with the guidance contained in the Small Business Guide.

Implementing these actions will significantly reduce the chance of you becoming a victim of cyber crime. To find out more, please visit **ncsc.gov.uk/smallbusiness**

Find out more

For further information, or to contact us, please visit:
www.ncsc.gov.uk

@ncsc

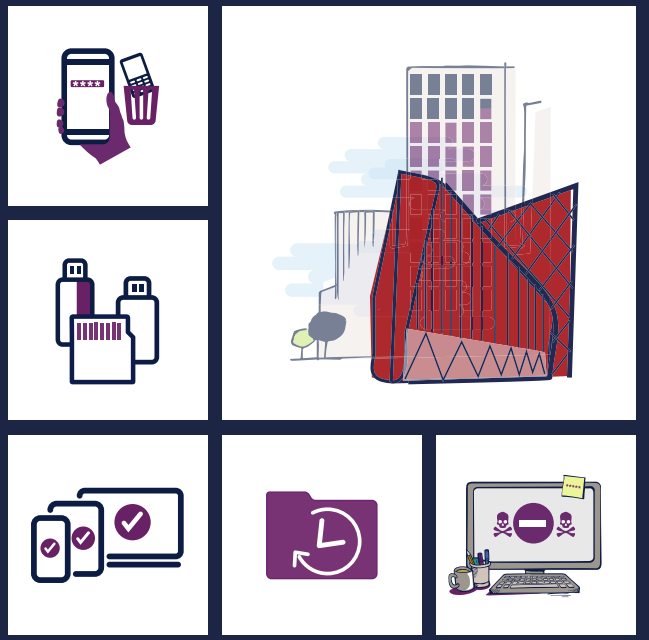
Information correct at time of publication – February 2018

National Cyber Security Centre
a part of GCHQ

National Cyber Security Centre
a part of GCHQ

Cyber Security:

Small Business Guide Actions



How to improve cyber security within your organisation – quickly, easily and at low cost.

Policy actions

These actions should be carried out by staff responsible for determining the overall cyber security policy.

- ☐ Identify and record essential data for regular backups.
- ☐ Create a password policy.
- ☐ Decide what access controls your users need so they can access only the information and systems required for their job role.
- ☐ Decide what staff need access to USB drives
- ☐ Sign up to threat alerts and read cyber local advice e.g. briefing sheets/threat reports from www.actionfraud.police.uk/signup.
- ☐ Create an inventory of approved USB drives and their issued owners, and review whether the ownership is necessary periodically.

Technical actions

These actions should be carried out by technical staff responsible for the setup and configuration of devices, networks and software.

- ☐ Switch on your Firewall.
- ☐ Install and turn on Anti-virus software.
- ☐ Block access to physical ports for staff who do not need them.
- ☐ Consider making a password manager available to your staff to secure their passwords. Review the star ratings before choosing one from an app store.
- ☐ Ensure data is being backed up to a backup platform e.g. portable hard drive and/or the cloud.
- ☐ Set automated back-up periods relevant to the needs of the business.
- ☐ Switch on password protection for all available devices. Change default passwords on all internet-enabled devices as per password policy.
- ☐ Install and turn on tracking applications for all available devices e.g. Find my iPhone.
- ☐ Enable two-factor authentication for all important accounts (eg email).
- ☐ Apply restrictions to prevent users downloading 3rd party apps.
- ☐ Install the latest software updates on all devices and switch on automatic updates with periodic checks.
- ☐ Ensure all applications on devices are up to date and automatic updates have been set to download as soon as they are released. Schedule regular manual checks on updates.
- ☐ Set up encryption on all office equipment. Use products such as Bitlocker for Windows using a Trusted Platform Module (TPM) with a PIN, or FileVault (on mac OS).

Training and awareness actions

These actions should be carried out by staff responsible for implementing staff training and awareness.

- ☐ Provide secure physical storage (eg a locked cupboard) for your staff to write down and store passwords.
- ☐ Create a Cyber Security training plan that you can use for all staff.
- ☐ Include details of your ‘Password’ policy explaining how to create a non-predictable.
- ☐ Include how to spot the obvious signs of phishing.
- ☐ Include details of your reporting process if staff suspect phishing.
- ☐ Include details on how your business operates and how they deal with requests via email.
- ☐ Include details of Wi-Fi hotspot vulnerabilities and how to use alternative options (eg VPN/ Mobile network).