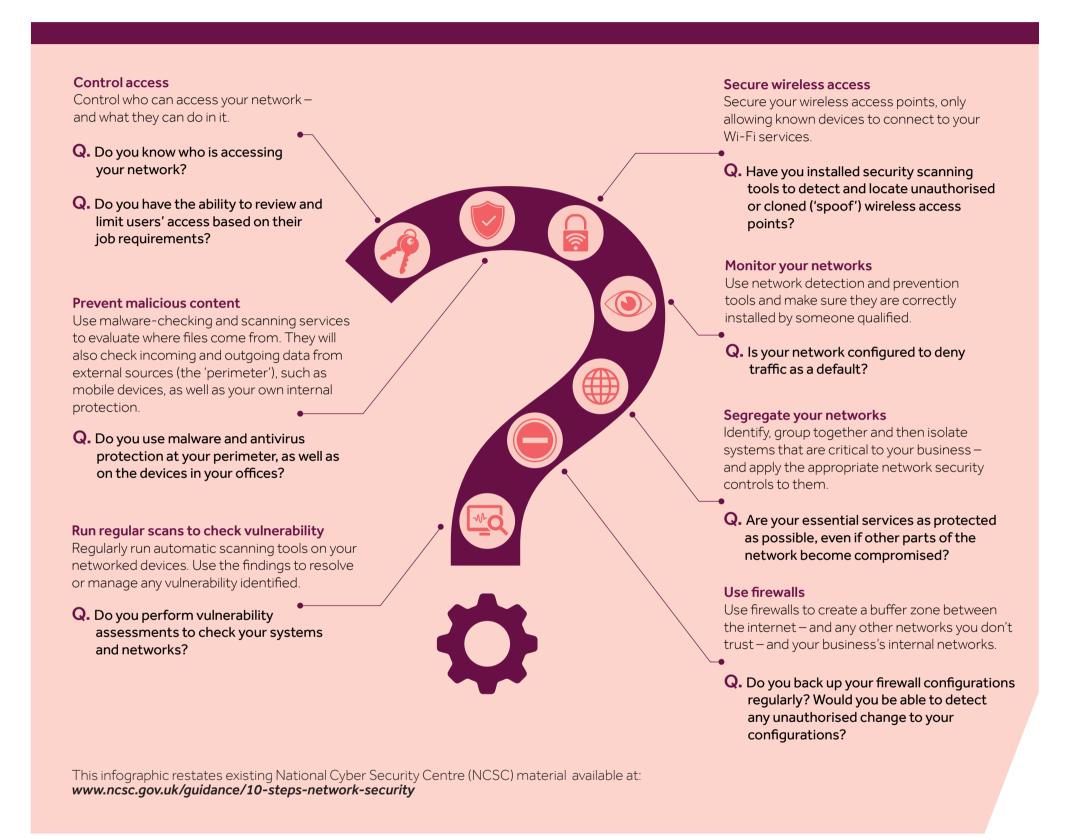# Network security - the basics

Effective cyber security starts with a secure network.
Help make your network secure by developing and implementing some simple policies and responses.

Control access
Control who can access your network – and what they can do in it.

Q. Do you know who is accessing your network?

Q. Do you have the ability to review and limit users' access based on their job requirements?

Prevent malicious content
Use malware-checking and scanning services to evaluate where files come from. They will also check incoming and outgoing data from external sources (the 'perimeter'), such as mobile devices, as well as your own internal protection.

Q. Do you use malware and antivirus protection at your perimeter, as well as on the devices in your offices?

Run regular scans to check vulnerability
Regularly run automatic scanning tools on your networked devices. Use the findings to resolve or manage any vulnerability identified.

Q. Do you perform vulnerability assessments to check your systems and networks?

Secure wireless access
Secure your wireless access points, only allowing known devices to connect to your Wi-Fi services.

Q. Have you installed security scanning tools to detect and locate unauthorised or cloned ('spoof') wireless access points?

Monitor your networks
Use network detection and prevention tools and make sure they are correctly installed by someone qualified.

Q. Is your network configured to deny traffic as a default?

Segregate your networks
Identify, group together and then isolate systems that are critical to your business – and apply the appropriate network security controls to them.

Q. Are your essential services as protected as possible, even if other parts of the network become compromised?

Use firewalls
Use firewalls to create a buffer zone between the internet – and any other networks you don't trust – and your business's internal networks.

Q. Do you back up your firewall configurations regularly? Would you be able to detect any unauthorised change to your configurations?

This infographic restates existing National Cyber Security Centre (NCSC) material available at:
www.ncsc.gov.uk/guidance/10-steps-network-security

Find out more

Cyber Security Information Sharing Partnership (CiSP)
www.ncsc.gov.uk/cisp

This is joint industry and Government initiative for exchanging information about cyber threats.

10 steps to cyber security
www.ncsc.gov.uk/guidance/10-steps-cyber-security

The National Cyber Security Centre's website gives more advice on how to protect your firm from a range of cyber and information threats.

FCA Cyber resilience
www.fca.org.uk/firms/cyber-resilience

Our website gives more information on cyber security and we update it regularly.

In partnership with

BANK OF ENGLAND
PRUDENTIAL REGULATION AUTHORITY

HM Treasury

National Cyber Security Centre
a part of GCHQ