Protect your organisation against cybercrime

What is Cyber Essentials? Cyber Essentials is a Government-backed and industry supported scheme to guide businesses in protecting themselves against common cyber threats.

Why is it important? Cybercrime is a worldwide issue that affects all organisations, of all sizes and in all sectors. It is vital all organisations focus on basic cyber hygiene, to ensure they are better protected from the most common cyber threats. The Cyber Essentials Scheme has been developed as part of the UK's National Cyber Security Programme and in close consultation with industry.

Whats involved in Cyber Essentials?

The main objective of the Cyber Essentials assessment is to determine that your organisation has effectively implemented the controls required by the Scheme, in order to defend against the most common and unsophisticated forms of cyber-attack.

There are two levels of certification that can be achieved.

Level 1 Cyber Essentials

Requires the organisation, with help from a practitioner, to complete a self-assessment questionnaire, with responses independently reviewed by an external certifying body.

Level 2 Cyber Essentials Plus

This covers the same requirements as Cyber Essentials but tests of the systems are carried out by an external certifying body, using a range of tools and techniques.

Why should you do Cyber Essentials?

You can prevent many attacks which use freely available software and techniques by implementing the Cyber Essentials five controls

You can identify areas for improvement, even if your organisation has a proven track record of good security, by going through the assessment

Your organisation can display the Cyber Essentials badge and demonstrate that it takes cyber security seriously by adhering to a widely-endorsed standard. In many cases, this badge is becoming a prerequisite in bidding for new contracts, particularly in the public sector.

ramsac
at the heart of IT

The 5 Cyber Essentials key controls

Cyber Essentials defines a set of five key security controls, which, when properly implemented, will better protect organisations, small and large, from attacks using software and techniques which are freely available on the open internet.

1

Boundary firewalls and internet gateways

Good set up of devices designed to prevent unauthorised access to or from private networks.

2

Secure configuration

Systems are configured in the most secure way.

3

Access control

Only those who should have access to systems have access, and at the appropriate level.

4

Malware protection

Virus and malware protection is installed and up-to-date.

5

Patch management

The latest support version of applications is used and all neccesary patches have been applied.

How can ramsac help?

ramsac have trained Cyber Essentials practitioners that can be bought in to undertake a gap analysis of where your network and general IT practices sit against the standard for Cyber Essentials certification. The result of the visit will be a gap report that we will then review with you to identify actions and agree any future project work, and then further review post activity with a view to preparing for external certification, ramsac can then refer you to an appropriate 3rd party certifier.

For more information on Cyber Essentials and how you can get your organisation certified contact ramsac on 01483 412040, email cybersecurity@ramsac.com or visit www.ramsac.com

ramsac
at the heart of IT