Protecting SMBs with Cyber Essentials Plus

In modern evolving cyber landscapes, organisations, regardless of their size, face a variety of threats that can compromise the security of their critical systems and sensitive information. Small, medium and large enterprises are all potential targets for cyber criminals seeking to exploit vulnerable services and applications. Common threats include phishing attacks, malware and ransomware campaigns, and data breaches. These threats not only have the potential to disrupt your key business operations but can also result in financial losses, reputational damage and legal repercussions.

For small and medium-sized enterprises, the challenge is often related to a lack of resources and a common perception of not being attractive to cyber criminals. Unfortunately, this is a misconception that attackers prey on, recognising that these companies often lack robust cyber security measures. Instances of ransomware attacks against small businesses have increased, with attackers recognising the potential for extracting ransom payments from organisations that handle sensitive information.

What is Cyber Essentials?

Cyber Essentials is a certification scheme developed by the National Cyber Security Centre (NCSC), which aims to mitigate common cyber threats and ensure organisations maintain a baseline level of cyber security across various industries.

By design, the scheme was developed to provide a set of fundamental cyber security controls that organisations are encouraged to implement, including:

- Secure Configurations
- Firewalls
- Access Control
- Malware Protection
- Patch Management

Organisations assess themselves against these five basic security controls, with a qualified assessor verifying the information provided.

Cyber Essentials Plus

Building on the Cyber Essentials framework, Cyber Essentials Plus provides a more rigorous approach by conducting an independent verification (audit) of an organisation's cyber security practices. This technical audit of in-scope systems includes:

- Internal vulnerability scans of servers and a sample of end-user devices to verify patch management and anti-virus/anti-malware practices are compliant.
- External vulnerability scans of all your public-facing Internet infrastructure to identify security vulnerabilities and to ensure good practices are followed.

It is awarded to organisations that not only meet the essential cyber security requirements but also demonstrate a higher level of security maturity.

To find out more or to speak to an expert contact us today

CONTACT US TO FIND OUT MORE

Or call: 0845 58 27001

This advanced certification offers a more robust assurance of an organisation's ability to withstand and respond to cyber threats, deepening their stakeholders, clients and partners' trust in them.

Process and Validity

All Cyber Essentials and Cyber Essentials Plus certificates have a 12-month expiration date. It can take 1 to 3 working days from submission for an organisation to become Cyber Essentials self-certified. A Cyber Essentials Plus assessment depends on an organisation's complexity and size, and can take 3 to 5 days after achieving Cyber Essentials self-certification.

How can Sapphire Help?

Sapphire is an IASME Approved Certification Body for Cyber Essentials and Cyber Essentials Plus and has a proven track record assisting organisations in becoming certified with the scheme.

IASME Cyber Assurance is a structured way for your organisation to implement and improve the way it secures information and offers assurance to the government, regulators, customers and vendors regarding your security posture.

Using Sapphire, we can guide you through certification for Cyber Essentials and conduct audits for Cyber Essentials Plus certification.

We will review your assessment of the controls of:

- Boundary Firewalls and Internet Services
- Security Configuration
- User Access Control
- Malware Protection
- Patch Management

As well as providing the following services for Cyber Essentials Plus assessment:

External Testing

Test whether an Internet-based opportunist attacker can hack into the applicant's system with typical low-skill methods

Internal Testing

Assess your defences against common attacks that originate externally but involve some form of an internal user action

Authenticated Vulnerability Scan of Devices

Identify missing patches and security updates that leave you vulnerable to easy exploits

Check Malware Protection on End User Devices (EUD)

Check all the sampled EUDs in scope benefit from at least a basic level of malware protection

Check the effectiveness of End User Devices (EUD) defences versus malware via Email and Web

Test whether or not EUDs are protected against malware delivered via email attachments or a website.

Check that multi-factor authentication (MFA) is enabled on cloud services

Verify that cloud services for normal and administrative users have been configured to make use of MFA

Check Account Separation

Verify that user accounts do not have excessive privileges assigned for normal business activities

	Cyber Essentials	Cyber Essentials Plus		
Service /Offering	All	Small Enterprise <100	Medium Enterprise <500	Large Enterprise >1000
Review of Self-Assessment For Cyber Essentials	✓	✓	✓	✓
• Boundary Firewalls & Internet Services	✓	✓	✓	✓
• Security Configuration	✓	✓	✓	✓
• User Access Control	✓	✓	✓	✓
• Malware Protection	✓	✓	✓	✓
• Patch Management	✓	✓	✓	✓
External Testing		✓	✓	✓
Internal Testing		✓	✓	✓
Vulnerability Scan		✓	✓	✓
Verify EUD Defences (Email & Website)		✓	✓	✓
Verify MFA for cloud-services		✓	✓	✓
Check Account Separation		✓	✓	✓

To find out more or to speak to an expert contact us today

CONTACT US TO FIND OUT MORE

Or call: 0845 58 27001