LAN SUPPORT

IT Service Excellence 30 Years 1996 -2026

# Cyber Essentials 2026: A Complete Guide for SMBs

Everything you need to know to get certified, stay compliant, and protect your business

# What is Cyber Essentials Certification?

Cyber Essentials is a UK government-backed cybersecurity certification designed to help organisations protect themselves against the most common cyber threats.

It focuses on five key areas of your IT setup that, when properly secured can prevent the vast majority of basic cyber attacks.

Just as importantly, certification provides a clear, recognised way to demonstrate to clients, suppliers, and other stakeholders that your business has solid data protection measures in place. It turns your internal security practices into an external signal of trust, something that's increasingly expected when handling sensitive information or working within a supply chain.

Rather than requiring complex or expensive solutions, Cyber Essentials is about getting the fundamentals right such as keeping systems up to date, controlling access to data, and protecting devices from malware.

There are two levels of certification:

**Cyber Essentials** A self-assessed certification, verified externally
**Cyber Essentials Plus** A more advanced level that includes hands-on technical testing

For many small and medium-sized businesses, Cyber Essentials acts as a practical starting point for improving security. It provides a clear framework to follow, while also demonstrating to clients, partners, and suppliers that your business takes cybersecurity seriously.

**In today's environment, it's increasingly seen as the minimum standard, not just for staying secure, but for staying competitive.**

# Why Get Cyber Essentials Certified?

Cyber Essentials certification helps protect your business against the most common cyber threats by ensuring the basics of your IT security are done properly.

Beyond protection, it also acts as a recognised signal to clients, suppliers, and stakeholders that your organisation takes cybersecurity seriously and has appropriate safeguards in place.

### Win more business

Many organisations, particularly in regulated industries, now require Cyber Essentials as part of their supplier due diligence.

### Meet compliance and contractual requirements

Certification is often a prerequisite for working with larger companies or public sector organisations.

### Reduce risk without overcomplicating things

It focuses on practical, high-impact controls rather than complex or costly solutions.

### Build trust with clients and partners

It provides a recognised, external validation of your security posture.
Why it matters more in 2026

Several trends are making Cyber Essentials more important than ever:

- Increased pressure from supply chains
- Rising cyber threats targeting SMEs
- Attackers increasingly see smaller businesses as easier targets, particularly where basic controls aren't in place
- Greater scrutiny around data protection
- Cybersecurity is becoming a business differentiator

**In short, Cyber Essentials isn't just about security. It's about trust, credibility, and staying competitive in an increasingly security-conscious market.**

# The 5 Cyber Essentials Controls

Cyber Essentials is built around five core technical controls. These are the fundamental security areas your organisation must get right in order to achieve certification.

Rather than relying on complex or expensive security tools, the scheme focuses on practical, high-impact measures that significantly reduce the risk of common cyber attacks.

### 1. Firewalls

Firewalls create a barrier between your internal network and the internet, helping to block unauthorised access and suspicious traffic. They are a first line of defence in keeping your systems secure.

### 2. Secure Configuration

This involves ensuring devices and systems are set up safely from the start. It includes removing unnecessary software, disabling unused features, and reducing settings that could create vulnerabilities.

### 3. Access Control

Access control ensures that only the right people can access the right data and systems. This typically includes strong password policies and multi-factor authentication to reduce the risk of unauthorised access.

### 4. Malware Protection

This control focuses on preventing, detecting, and removing malicious software. It includes antivirus and anti-malware tools, as well as safe browsing and email protections.

### 5. Patch Management

Patch management is about keeping software and devices up to date. Regular updates fix known security vulnerabilities, closing gaps that attackers could exploit.

**Individually, each control addresses a common weak point in business IT systems. Together, they form a baseline security standard that protects against the most frequent types of cyber attack.**

# Cyber Essentials vs Cyber Essentials Plus

There are two levels of Cyber Essentials certification: Cyber Essentials and Cyber Essentials Plus. Both are based on the same five controls, but they differ in how your security is assessed.

Importantly, Cyber Essentials is a prerequisite for Cyber Essentials Plus. You must achieve the standard Cyber Essentials certification before progressing to the Plus level.


Cyber Essentials is the entry-level certification. It involves completing a detailed questionnaire about your IT setup, which is then reviewed by an external certification body.

It's designed to confirm that your organisation has the essential security controls in place and is a good fit for businesses looking to demonstrate a recognised baseline of cybersecurity.


Cyber Essentials Plus builds on the standard certification by adding independent technical verification.

Instead of relying solely on a questionnaire, your systems are tested by security professionals to confirm that the controls are properly implemented and effective in practice.

This provides a higher level of assurance and is often required by organisations handling more sensitive data or working in regulated environments.

# Cyber Essentials Costs in 2026

Cyber Essentials costs vary depending on the size of your business, your current IT setup, and the level of support you need. It's useful to think of the cost in two parts: the certification fee itself, and the work required to get your business ready.

## 1. Certification cost

The certification fee is set in bands based on company size and is relatively affordable for most SMEs. However, this is only part of the overall cost. Your existing IT security setup, the complexity of your environment, and whether you handle it internally or with support.

## 2. The real cost

The main cost is usually the time and effort involved in meeting the requirements, including reviewing your current setup, fixing gaps against the five controls, and completing and submitting the assessment.

Without experience, this can take longer than expected and may lead to failed submissions.

## 3.How we make it simple

At LAN Support, we remove the risk and uncertainty from the process:

• We make sure your setup meets the required standard before submission, so there are no surprises.

• Cyber Essentials certification is included free for the first year for new customers.

• You're guaranteed to pass first time when on one of our plans.

**Want to get certified the easy way? Get in touch:**
**01483 413360| stephenj@lansupport.co.uk**