CyberSmart

CYBER ESSENTIALS FOR UK BUSINESS

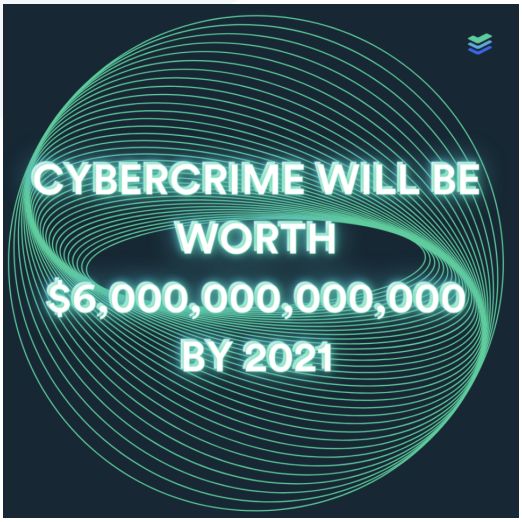
CONTENTS

WELCOME TO CYBERSMART

CyberSmart cuts the Cyber Essentials certification process from months to hours, while also checking, fixing, and monitoring compliance around the clock.

Cyber Essentials for UK Business

Cybercrime is on the rise. At the time of writing, it's more profitable ($600bn p/a) than the global illegal drugs trade and set to cost the world $6 trillion annually by the end of 2021.

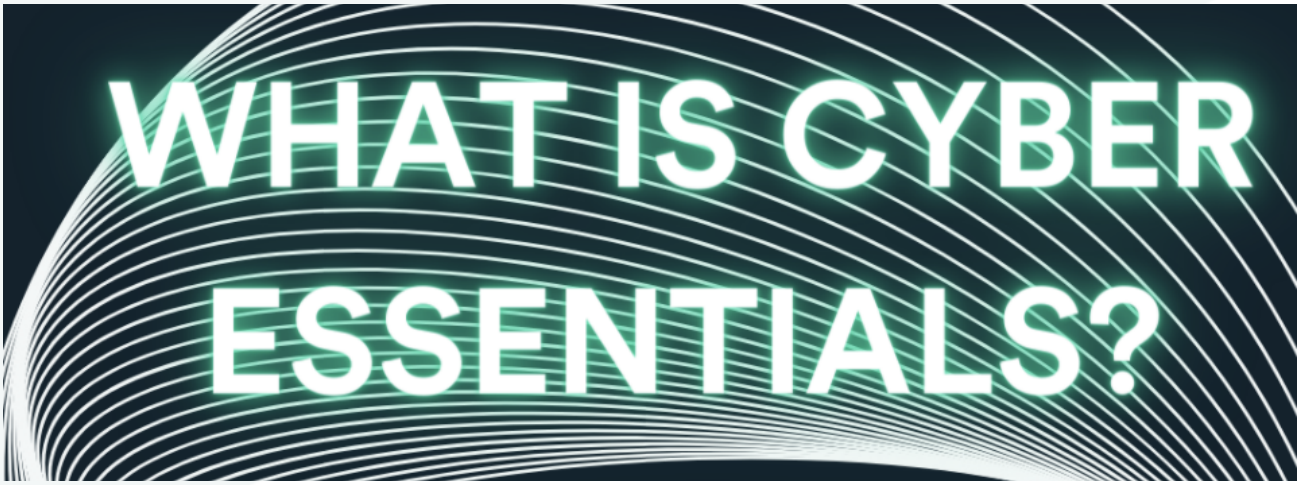


So it's safe to say that cybercrime is one of the biggest threats to any business operating today. But until recently, awareness of the threat to SMEs has been low.

Despite attacks on small businesses now accounting for 58% of all cybercrime, many businesses still feel they're too small to be targeted, leaving them vulnerable.

Even for those SMEs who are conscious of the risks, stretched budgets and a lack of specialist knowledge can make adequate protection feel hopelessly out of reach. However, protecting your business doesn't have to involve cyber expertise, the latest technology or costly consultants.

In this guide, we'll look at how Cyber Essentials certification can provide your business with the basics needed to protect itself from most cyber threats.



Back in 2014, the British government became aware of the enormous risks posed to businesses – particularly SMEs – by cyberattacks. They also recognised that most of these risks were easily preventable. All companies needed to do was follow a set of basic security measures.

So, in response, they created the Cyber Essentials scheme. The scheme covers the essential actions every business should take to ensure its digital security and protection from cyberattacks. Think of it as 'cyber hygiene' – a bit like washing your hands, brushing your teeth or wearing a face mask.

The scheme assesses five key criteria:

- Is your internet connection secure?
- Are the most secure settings switched on for every company device?
- Do you have full control over who is accessing your data and services?
- Do you have adequate protection against viruses and malware?
- Are devices and software updated with the latest versions?

Once you've familiarised yourself with these basic controls and have them in place, Cyber Essentials requires you to fill out a questionnaire confirming all company devices meet the criteria. This is a self-assessment which you then sign and submit for review by a certification body.

Cyber Essentials Plus explained

Cyber Essentials Plus is the older, slightly more involved sibling of the standard certification. It has the same requirements as Cyber Essentials (you must have all five security controls in place) but differs in one crucial aspect.

While Cyber Essentials is self-assessed, Cyber Essentials Plus also includes an independent assessment carried out by a licensed auditor.

After you've completed the self-assessment portion of the certification, an auditor will either visit you onsite or remotely access your network and manually check for the five Cyber Essentials controls.

This provides you with absolute assurance that your cybersecurity is up to scratch. And customers don't have to take your word that you're cyber secure – they can rely on the expertise of a professional.

Cybercriminals are increasingly targeting SMEs. In the UK alone, small businesses are subject to 10,000 attacks every day.

06

Why is Cyber Essentials important for SMEs?

Good cyber hygiene is crucial for any organisation. So what makes Cyber Essentials certification particularly important to smaller businesses?

Growing risk

The UK economy is populated by thousands of SMEs. In fact, according to the Federation of Small Businesses, SMEs account for 99.9% of the business population. So, it's no exaggeration to say that the dynamism and agility of small businesses are the driving force behind the UK economy.

However, the qualities that make SMEs so valuable also leave them vulnerable to attack. Cybercriminals are increasingly targeting SMEs. In the UK alone, small businesses are subject to 10,000 attacks every day.

The reason for this is simple. Large enterprises have the resources to purchase the best cybersecurity tools and weather any attacks that do happen, SMEs typically don't. Add to this that many SMEs are part of a supply chain for larger, higher-profile organisations and it's not hard to see why they're such an enticing target for cybercriminals.

And things are only getting worse. With many businesses switching to permanent or temporary remote working in the wake of the COVID-19 pandemic, cybercriminals have been given an easy target. So much so, that 91% of global businesses have seen an increase in cyberattacks as a result.

Workers using their own devices, networks and software are far more vulnerable than they would be at work. According to a report from BitSight, home office networks are 3.5 times more likely than corporate networks to be infected by malware.

Government Contracts

Public sector work is often an important source of revenue for many SMEs, particularly in light of the recent COVID-19 pandemic.

But to bid for much of this work, you'll need to be Cyber Essentials certified. Cyber Essentials is mandatory for any government contract that involves the handling of personal data.

Certification is required for:

- Handling the personal information of any UK citizens; i.e. bank details or home addresses
- Processing or handling the personal information of any government employees, ministers, or advisors; i.e. payroll or expenses information
- Delivering IT products or services designed to store, process, or transfer data at an official level

And this doesn't just apply to civic projects. The Ministry of Defence (MoD) requires all organisations within its supply chain to be Cyber Essentials compliant. This means that even if your business doesn't work directly with the MoD, Cyber Essentials is still required if your partners or customers do.

The CyberSmart desktop and mobile app ensure constant compliance in your institution

Customer assurance

As public awareness of the threat of cybercrime and the consequences of data breaches grows, so too have demands on businesses. It's no longer enough to tell your customers that your business takes cybersecurity seriously, you need to prove it.

Cyber Essentials certification provides clear, government-backed proof that your business is safe to work with. This not only offers assurance to your current customers but also gives you an edge when competing for new ones.

How do you get Cyber Essentials certified?

Achieving Cyber Essentials certification is a simple, step-by-step process.

1. Submit a self-assessment covering the five criteria through an online portal.
2. A certification body assesses and grades the application.
3. If graded as a 'fail', the points that didn't pass must be addressed and the assessment taken again.
4. If graded as a 'pass', that's it. You're Cyber Essentials certified and able to demonstrate your credentials to customers, partners and suppliers.

The CyberSmart desktop and mobile app ensure constant compliance in your institution

Why CyberSmart?

We do Cyber Essentials certification a little differently. Getting certified shouldn't be costly, complex or frustrating. So, we make it simple.

- Unlimited expert guidance to ensure you pass first time
- Certification within 24 hours
- £25k free cyber insurance with certification

However, much like an MOT, Cyber Essentials certification only guarantees your business is working safely on the day of assessment. How do you stay compliant the rest of the time?

This is where the CyberSmart platform comes in.

CyberSmart monitors all your business's devices 24/7. It checks for the most up-to-date applications, operating systems, firewalls, security measures and compliance with Cyber Essentials – protecting your business against 98.5% of cybersecurity threats.

All of this is available in the platform's smart dashboard. This allows you to check the status of individual employee's devices, resolve any security issues in-app and distribute security policies across the entire business.

CyberSmart can even improve understanding of cybersecurity within your business, with engaging training modules delivered straight to employees' devices.

The CyberSmart desktop and mobile app ensure constant compliance in your institution

CyberSmart

"CyberSmart's monthly subscription is perfect for those in the start-up space. Shelling out thousands of dollars in one go is tricky for a small business. The subscription model makes CyberSmart's tools accessible to organisations in a similar position to us when we first started."

- Ben Pook, Director of Play Verto

Trustpilot

cybersmart.co.uk