exertis | ENTERPRISE

CYBER ESSENTIALS

Cyber Essentials for Education

A simple guide to Cyber Essentials for schools, universities, and further education providers.

CONTENTS

03

Why is good cybersecurity so important for education providers?

Schools, universities, and further education providers might not seem an obvious target for cybercriminals. There are far more lucrative and high-profile targets out in the wider economy, so why attack a school or college?

Unfortunately, education providers' lower profile isn't enough to protect them from cybercrime. In May 2020, Microsoft Security Intelligence found that 61% of nearly 7.7 million malware encounters came from those in the education sector.

There has also been a rapid rise in the number of cyberattacks on schools, universities, and colleges. September 2020 and February 2021 saw a spike in ransomware attacks on the sector, prompting the National Cyber Security Centre (NCSC) to urge the education providers to take action to better protect themselves.

It's not hard to understand the NCSC's concern. For those education providers who do suffer a breach, the consequences can be severe. For example, the government's 2021 cybersecurity breaches survey found that a third of schools that suffered a breach lost control of their systems, data, or money.

For institutions with already stretched budgets, being required to pay a ransom for the return of sensitive data spells potential disaster. Meanwhile, any systems outages caused by a successful attack could prove detrimental to students' education – particularly during the COVID-19 pandemic when most teaching has been virtual.

And this is before we even consider the long-term ramifications of a breach. Most education providers pride themselves on student safety and data protection. Any failure on that front risks the reputation of your institution and its draw for prospective students.

04

Why are cybercriminals targeting education providers?

We've covered why cybersecurity is so important to education providers, but you could be forgiven for wondering why cybercriminals target the sector at all. What is it about education that so appeals to the bad guys?

Firstly, educational institutions are, by their nature, hubs of sensitive data. And most institutions have a firm commitment to data protection. Cybercriminals are aware of this and also know that education providers have little choice but to pay out to get their data back. These two factors combined make the education sector a prime target for ransomware attacks.

On top of this, most cybercriminals are, at heart, opportunistic. And education providers offer a very tempting opportunity.

Studies show the education sector is one of the least well-protected. Last year, a hacker simulation test proved 100% successful in breaching 50 universities across the country. The test was able to access student and staff personal data, financial systems, and valuable research networks.

It's not just that schools, colleges and universities often lack sufficient defences to repel attacks, they're also filled with hundreds or even thousands of staff all using the internet. It only takes one misclick on a phishing email or bogus website to give cybercriminals access to a trove of sensitive data.

05

What is Cyber Essentials?

You've probably heard the phrase 'Cyber Essentials' mentioned before, but what is it?

Cyber Essentials is a government-backed certification scheme that covers the essential actions every organisation 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:

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

Once you understand these basic controls and have them in place, Cyber Essentials requires you to fill out a self-assessment questionnaire confirming your organisation's devices meet the criteria. You then sign and submit for review by a certification body. If all goes well, your organisation is passed and can consider itself secured to the UK government standard.

Key features

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

06

Cyber Essentials Plus

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 come to you 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 prospective students don't have to take your word that you're cyber secure – they can rely on the expertise of a professional.

Key features

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

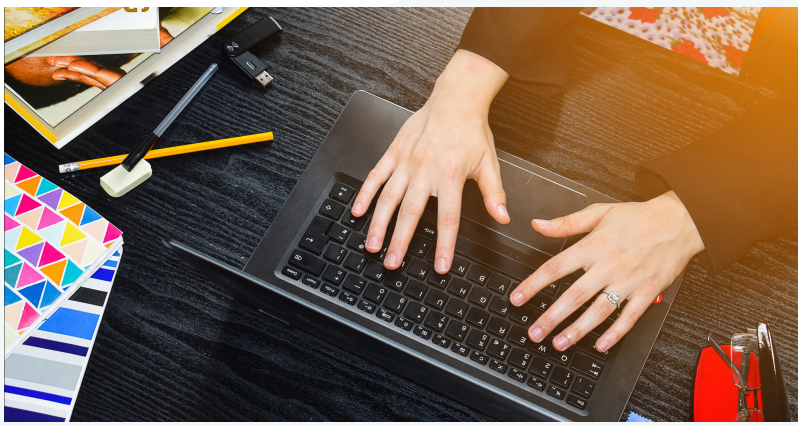
07

What are the benefits of Cyber Essentials?

You may need Cyber Essentials certification to qualify for certain types of funding (more on which later). However, the benefits go far beyond funding criteria.

According to research from Lancaster University, getting certified can protect your organisation from 98.5% of the most common cybersecurity threats. It's also a great indicator of your institution's commitment to security and data protection, helping boost your organisation's reputation among prospective students and their families.

Completing Cyber Essentials certification also has a long-term benefit. By putting in place the measures needed to complete the assessment, you'll also create a culture of cyber safety – helping to protect your institution against future threats.



Who needs Cyber Essentials?

Although every school, college, university or training provider could benefit from Cyber Essentials, there are a few specific instances where it's required.

Further education and training providers

In January 2020, the UK government included Cyber Essentials in its updated data security requirements for funding awards through the Education and Skills Funding Agreements (ESFA)

For the 2020 to 2021 funding year, any further education provider applying for ESFA funding must meet the requirements of the Cyber Essentials scheme. For the 2021 to 2022 funding year, this will increase to include Cyber Essentials Plus certification.

Who needs Cyber Essentials?

Schools

Cyber Essentials isn't compulsory for schools yet. However, this looks set to change in the near future with both the NCSC and certification body IASME, urging schools to consider certification.

Why wait for it to become compulsory? By getting certified today you'll not only be ahead of future funding requirements, you'll also ensure your school is protected and enhance it's reputation for data protection and student safety.

Universities

Much like schools, there's currently no requirement for universities to complete Cyber Essentials to qualify for funding. But, as universities continue to be targeted by cybercriminals, it's only a matter of time before this changes.

Again, it's worthwhile considering Cyber Essentials certification before it becomes a requirement for government funding. The same logic applies to universities as it does to schools. Getting certified will protect your institution from most cyberattacks and distinguish it from competitors as an organisation that takes data protection and cybersecurity seriously.

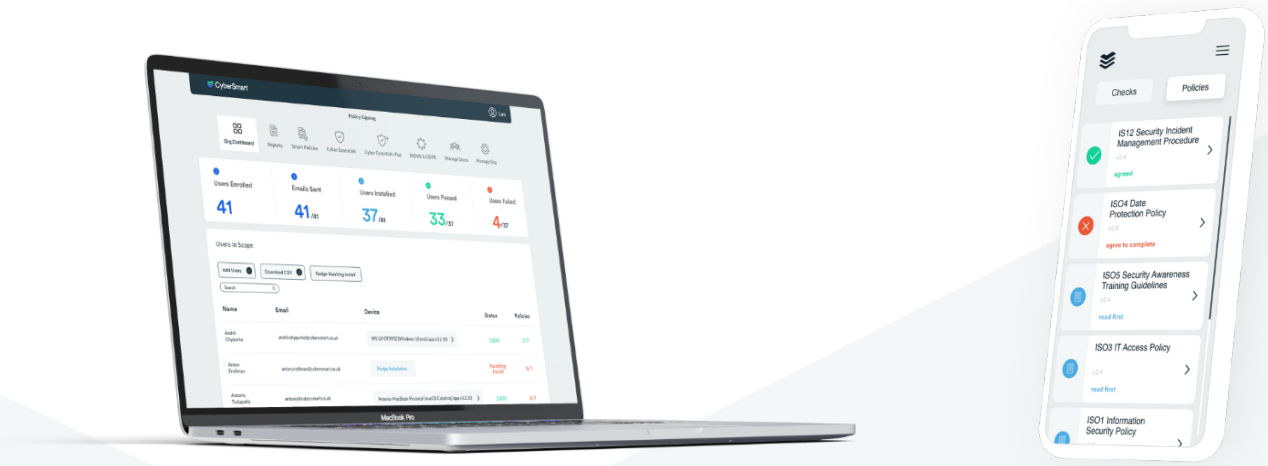
More than certification

CyberSmart offers the fastest, simplest path to certification on the market. But we don't stop there, because security is about more than certification.

With remote work and study fast becoming the norm, it’s never been more important that your staff can access systems and data safely from any device. Unfortunately, certification only guarantees protection at the time of assessment. So how do you ensure your people are working safely all the time, even if they're using personal devices?

The CyberSmart App does exactly that. Installable on any device, the app continually runs in the background, assessing security every 15 mins. If a device fails a security check, you’ll be notified via the CyberSmart Platform’s central dashboard and provided with step-by-step guidance on how to fix the issue.

In addition to security monitoring, the app also allows you to distribute cybersecurity policies to any device. So no matter where your staff are, they'll always have access to the guidance they need to stay safe.



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

CyberSmart provided us with a fantastic experience. Their automated app makes managing and keeping compliant with Cyber Essentials very easy. To get us certified, their team went the extra mile and helped us effectively with their simple and straight forward process. So I highly recommend using them if you want to get your cyber essentials certification in a trouble free method.

- Zein S.

Trustpilot

exertis | ENTERPRISE

Get In Touch

Contact: Grant Eaton
T: 01782 648100
M: 07920 364846
E: grant.eaton@exertis.co.uk
W: **exertis.co.uk/cybersmart-security**