central technology

Cyber Security

Our leading systems and solutions are embedded in our Managed IT Support to protect your business against costly data breaches. We see this as an integral part of our service to ensure our customers are safe from cyber threats.

Managed Cyber Security

Cyber Security is a fundamental part of modern organisations to protect the devices we use and the services we access from cyber attacks. These cyber attacks are usually aimed at accessing, changing, or destroying sensitive information and disrupting business processes. Every business is susceptible to a cyber-attack no matter the size of the organisation. We provide all the resources you need to ensure a resilient security posture, including proactive threat monitoring and incident response services as part of our Managed IT Support packages.

Don't risk your brand reputation

Brand loyalty through a strong cyber security position is paramount for customers today, and the shortest path to repeat business and recommendations.

Increase your productivity

Cyber attacks can slow networks and personal devices down to a crawl, making it virtually impossible for employees to work. By implementing a range of cyber security measures, you can drastically reduce violations and the downtime it takes to remedy the breach.

Protect your business

Both internal and external threats can bring your business to a standstill. We can ensure your data is protected against malicious attacks as well as corruption.

Can you afford a cyber attack?

As cyber attacks only continue to grow more sophisticated and complex every day, it's important to weigh the cost of dealing with one attack versus the value of taking preventative measures.

Ensure your business is compliant

In response to the increased cyber threats and exposure of sensitive data businesses face today, many regulatory bodies are setting standards to help protect organisations and their customers alike.

Start with a security review

Our Cyber Security review will highlight areas that will need remediation prior to applying for the Cyber Essentials certification. Following our review we'll provide you with an overview of the steps required for remediation and assist you in preparing to apply for the CE certification.

Vulnerability scans

We can scan your external entry points and main website for vulnerabilities. When we identify a potential concern, we carry out a corrective action and rescan, you will then get a report detailing any outstanding threats or corrective actions. We also recommend annual pen testing with an accredited assessor to ensure you are aware of your security vulnerabilities.

Upskill your workforce with user awareness security training

We have developed an online training platform that consists of short videos covering a range of topics including Cyber Security, Microsoft Excel, Teams and Exchange as well as softer subjects.

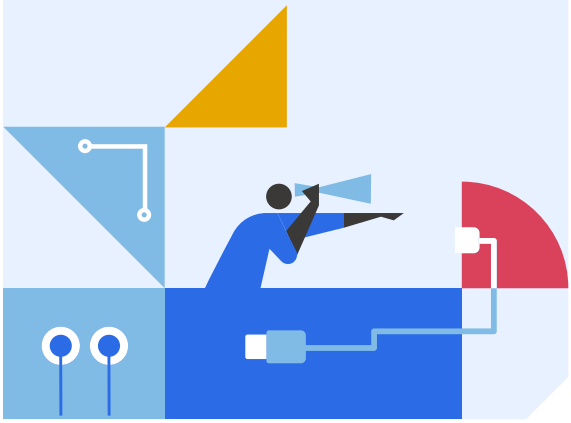
Two-factor authentication

External entry points to your infrastructure (such as Office 365 and onsite services accessible remotely) should be protected by two-factor authentication to ensure that external access is limited to person in possession of both a password and a token.

Cyber Security Review

Cyber Essentials is a Government backed scheme that helps protect your organisation against the most common cyber attacks. Our cyber security review will highlight areas that will need remediation prior to applying for the Cyber Essentials certification. Following our review we'll provide you with an overview of the steps required for remediation and assist you in preparing to apply for the CE certification. Our advice, in the shape of five technical controls, is easy to implement and designed to guard against these attacks.

What is Cyber Essentials?



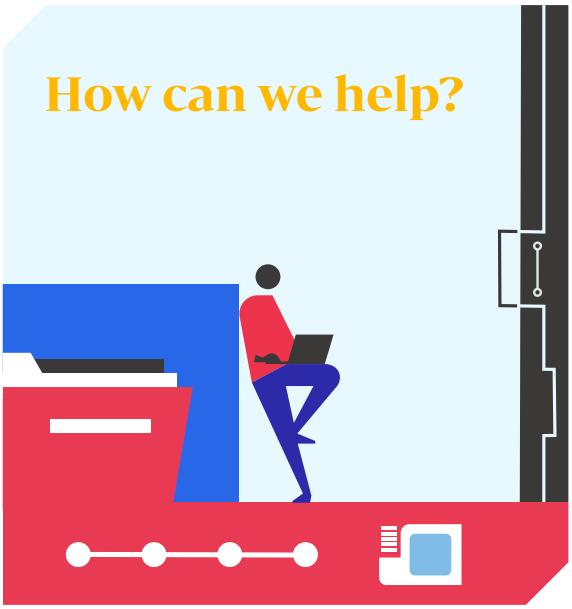
Cyber Essentials offers a simple and effective level of assurance for businesses of all sizes and comes in two levels: Cyber Essentials and Cyber Essentials PLUS. The programme sets out 5 key technical controls to help your business protect your business against the most common cyber threats. The Cyber Essentials certification aims to reduce an organisations' risk of attack from internet-borne threats by around 80%.

When helping your business achieve either of the Cyber Essentials certifications, which provide a certification that a business has the tools in place to mitigate the risk from common cyber threats.

We first carry out an in-depth strategic review of your current IT infrastructure to identify any current or potential risks whilst understanding future IT requirements of your business. This is conducted with the goal of creating an overall IT strategy to ensure you pass the Cyber Essentials certification.

The presented IT plan could help you achieve your business goals in the future whilst ensuring the immediate necessary work is carried out to achieve the Cyber Essentials accreditation.

How can we help?



CYBER ESSENTIALS

WEBROOT an opentext company

Why your business should consider a Cyber Essentials accreditation

A security promise to new & existing customers

Displaying the Cyber Essentials certification badge on your website and appearing in the 'Cyber Essentials' online directory is an important way to reassure your customers that their data, money and own cyber security is in safe hands. Not only can you reassure your own customers that you're actively working to secure your IT against cyber attacks, any potential new business you attract will also have peace of mind that they will be working with a business who prioritises being cyber secure with top-level cyber security measures in place.

Contractual requirements for Cyber Essentials certification

If your organisation is looking to win public sector deals, Cyber Essentials is a mandatory requirement for some Government and supplier contracts.

Have a clear picture on your organisation's cyber security level

Having knowledge of your organisations cyber security level can ensure your business stays 'cyber security ready' which can lower your risk of major disruption in case of a cyber attack as you can make informed decisions on how to improve your security.

Avoid the impacts of serious cyber attacks

Cyber Essentials is the UK Government's answer to creating a safer internet space for businesses of all sizes, across all industries. Created and operated by the National Cyber Security Centre (NCSC), Cyber Essentials is considered the best first step to a more secure network, protecting you from 80% of the most basic cyber security breaches.

Protect customer and employee information

If your business has an IT infrastructure that collects, stores and/or uses customer and employee information, your organisations IT system can be vulnerable to attack. Cyber Essentials is the first line of defence against these basic but potentially devastating attacks on private information.

5 Ways to stay Cyber Secure

01 Firewall protection for network traffic

A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules. If your firewall scans malicious code as a security risk, it will be prevented from entering the network or reaching your device.

02 Keep your devices up-to-date

Updates for devices and softwares often contain new features, fixes for bugs and performance improvements. They may also contain security patches and new security features that will fix known flaws in products that would leave your devices vulnerable.

03 Control who has access to your data

Controlling access is a way of guaranteeing that users are who they say they are and that they have the appropriate access to company data. Access control is a selective restriction of access to data, without authentication & authorisation, there's no cyber security.

04 Be aware of suspicious emails and pop-ups

You can lower your risk of cyber attacks by being vigilant of suspicious emails, pop-ups or links that could leave your device compromised to malware & other viruses. Internal cyber security training could help with this.

05 Secure device settings

To keep your information secure from potential security risks, it's important to take a close look at the security & privacy settings on all of your devices, accounts & apps. Your should only install trusted software & restrict who can install software and change device settings to keep your settings secure.

ct.uk T | 01246 266 130 E | info@ct.uk