Cyber Essentials

HM Government

CYBER ESSENTIALS

Cyber Essentials is scheme and a standard backed by UK Government to address malicious risks originating from the internet, typically termed Cyber Threats. Created by the Government for UK businesses, so that they know where to start and what to do. The net result is to reduce the risk of becoming a victim of internet fraud and cyber-attack, and to become a more robust and confident business in the complicated and fast moving world of commerce.

You don't have to trade online to take advantage of the scheme, just about any business that uses internet banking for instance has an asset that the cyber criminals would value stealing. And much too often it is the small business, or the organisation that does not think it has anything worth stealing. They typically have less resources and more priorities, all making easy them an easy target for a Cyber-criminal.

The scheme comprises of two phases: Cyber Essentials and Cyber Essentials+

Cyber Essentials comprises a self-assessment questionnaire to help businesses readily understand the controls and actions they should address.

Cyber Essentials+ comprises the questionnaire and an onsite technical assessment to measure the controls and their effectiveness against a cyber-attack.

Receive FREE Cyber Liability Insurance for the first 12 months after passing the self-assessment. Thanks to our affiliation with the accreditation body IASME, this is available to any UK domiciled organisation with less than £20m annual turnover and covers them up to £25,000.

"Daily, over one million victims of cybercrime per day in the UK"
"Cyber crime UK cost £27 billion*"

Birkenhead Varnish producer AEV victim to a cyber-attack, results £100k being transferred from bank account.

Truffles – A small Bakery in Surrey and Home Counties falls victim to a cyber-attack and is defrauded of £19k.

*Source: Hacking Britain report

Cyber Essentials advocates the following **5 control themes** to reduce 80% of internet threats

1. **Boundary firewalls and internet gateways** - devices designed to prevent unauthorised access from public (untrusted) networks — Keep the threat outside of the trusted network
2. **Secure configuration** – systems are configured in the most secure way for the needs of the organisation — Diminish the possibility for the threat to succeed
3. **Access control** – fitting and appropriate access to systems with an approach least privilege allocation. — Reduce the ability for the threat to propagate
4. **Malware protection** – ensuring that virus and malware protection is installed, operational and effective — Block automated threats targeting users and
5. **Patch management** – using supported version of os's & applications are used, and all necessary patches are applied. — Obstruct and nullify the export opportunity

CST

Tel: 0207 621 7836
Email: info@cstl.com
Web: www.cstl.com