Lancashire Cyber Foundry

Is Your Business Ready for Cyber Essentials

READ TIME: 2 MINS

AUDIENCE: BUSINESS & TECHNOLOGY

WHAT IS CYBER ESSENTIALS

The National Cyber Security Centre's (NCSC) Cyber Essentials scheme is a government backed certification that is designed to help you to protect your organisation. This is through mitigating the potential risks of the most common cyber threats, via ensuring the implementation of the fundamental cyber security controls and protection methods.

The required security controls are categorised into 5 basic technical themes, including:

- Firewalls
- Secure Configuration
- User Access Control
- Malware Protection
- Security Update Management

WHY IS IT NEEDED

By implementing the necessary protection measures to become compliant with the requirements of the Cyber Essentials scheme, your organisation will be more protected against the ever-growing threat of cyber-attacks. For this reason, Cyber Essentials is considered the best first step in securing your organisation, protecting you from approximately 80% of the most common cyber-attacks, for example phishing, malware, ransomware, or network attacks.

In addition, achieving the Cyber Essentials certification builds trust with the customers, and boosts the overall reputation of your organisation. This is because it will reassure customers that you are taking a proactive stance to cyber security, through demonstrating your commitment to protecting your data and network infrastructure.

Moreover, becoming compliant with the Cyber Essentials scheme will attract and open new business. As an example, having the crucial cyber security controls in place can allow an organisation to apply for government led contracts, involving the secure handling of sensitive information.

European Union
European Regional Development Fund

NORTHERN POWERHOUSE HM Government

Lancaster University

MAKING A START

The following section covers some frequently overlooked security issues that must be considered in order to obtain Cyber Essentials.

- Firewalls: Ensure that the firewall is enabled on all devices androuters, as well as configured to block any unauthorised incoming connections by default.
- Secure Configuration: Remove or disable any unused user accounts. Uninstall any unnecessary software and applications. Disable the AutoRun feature on all devices.
- User Access Control: Have a clear, documented account creation and approval process. Have an appropriate password policy in place and implement Multi-Factor Authentication (MFA) where possible. Only perform admin activities on an account with admin privileges (i.e. no emails or internet browsing) and remove special privileges when no longer required.
- Malware Protection: Ensure that all devices are protected with anti-virus software, and it automatically scans files and pages.
- Security Update Management: Remove unsupported software and applications. Apply all updates within 14 days of release.

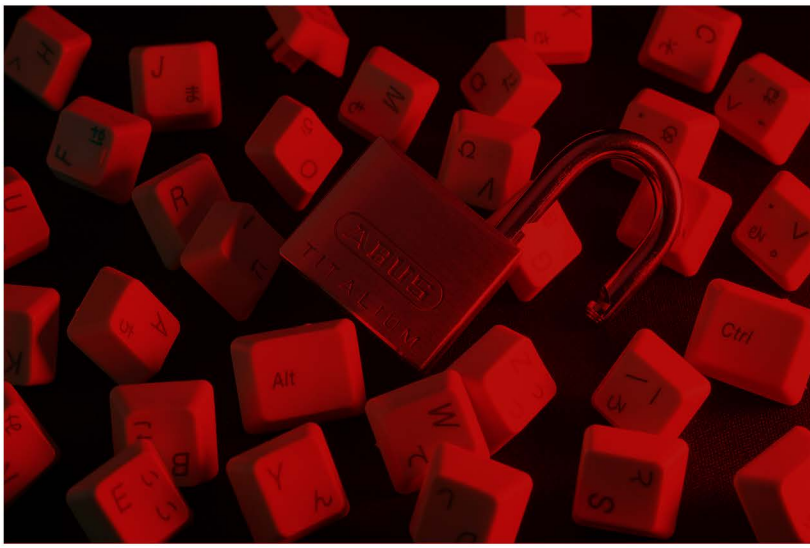
ADDITIONAL RESOURCES

To find out more about the Cyber Essentials scheme, the NCSC website provides an overview of the certificate and offers answers to the frequently asked questions.

In addition, a detailed list of each requirement within the 5 control themes are provided in a detailed PDF file, and the Cyber Essentials Readiness Toolkit can be used to create a personal action plan, to receive guidance on the next steps to meet each requirement.

To find out more visit the NCSC website:

https://www.ncsc.gov.uk/



ABOUT US

Lancashire Cyber Foundry

The Lancashire Cyber Foundry runs a programme designed to support businesses facing cyber challenges in Lancashire. Digital Innovation support is part of this programme but there is also business strategy support available too which includes specialised workshops to help businesses innovate and grow.
ITo find out more about how your business can access support and register on one of the upcoming cohorts contact us at:

cyberfoundry@lancaster.ac.uk