SME

A SECURE FUTURE

UNDERSTANDING AND REDUCING RISKS WITH A CYBER SECURITY AUDIT

inTEC BUSINESS

0345 565 1767
info@intecbusiness.co.uk
intecbusiness.co.uk

REDUCE THE RISKS

As a Microsoft Gold Partner, we can offer helpful advice and implement the right solutions to protect the devices you use and the data you manage in your business every day. We'll ensure that the services you access are safe. We can also help you to stop unauthorised access to the vast amounts of confidential information you store on your device and online.

Even with the increase in cyber-attacks over recent years, many small and medium sized business are still reluctant to take action by investing in a effective security solution. Don't assume that, if you have a relatively small business, hackers won't attack. Our experience shows that the opposite is in fact the case: to target as they generally do not have appropriate security solutions in place nor a dedicated internal team to manage cyber security. **43%* of cyber-attacks are aimed at small businesses!**

*Source: Cyber Security Statistics: Numbers Small Businesses Need To Know - Small Business Trends

THE STATS DON'T LIE

The stats are compelling and speak for themselves. We're here to ensure that your business does not become the next victim of cyber-attack. So whether you would like us to review the security of your IT systems in general or you are interested in a specific element (e.g., remote worker device security, password protection, data backup...) get in touch to book your Cyber Security Audit.

EXAMPLES OF CYBER SECURITY ATTACKS

Phishing attacks

This is an attempt to steal sensitive information, usually usernames, passwords, credit card numbers, bank account information and date of birth. The phishing attempts, usually originate from an email pretending to be a bank, a delivery firm or even a relative.

Malware attacks

This is malicious software which infects your computer. It can attempt to steal information or even encrypt your files with ransomware to extort money from the business.

Ransomware

A particularly disruptive form of malware, which encrypts your data and systems with an attempt at extorting money for the release of this data.

Weak passwords

It's important to use complex passwords which aren't easy to guess and aren't used on any other systems, particularly on the internet. If one password is compromised and published on the internet, then hackers will have access to all the other systems.

Insider threats

Unfortunately, many cyber incidents occur from within, these could be from disgruntled employees, careless workers or even a malicious insider. It's important to ensure that employees only have access to the information they require and cyber awareness training, given to employees on a regular basis.

Backups

If you lose access to your systems, it's crucial this information is backed up, ensuring the system holding the backups is secure, offsite and detached from your systems. Having good backups will enable you to recover quickly from a ransomware attack, negating the need for expensive extortion attempts.

OUR CYBER SECURITY SOLUTIONS

CYBER SECURITY HEALTH CHECK

A cyber security health check will help you identify your organisation's weakest security areas. We'll recommend appropriate measures to mitigate your risk and conduct vulnerability scans of critical infrastructure LPS & website/URL.

CYBER ESSENTIALS AUDIT

Cyber Essentials is a government-backed, industry supported scheme to help organisations protect themselves against common cyber attacks. Choose from Cyber Essentials or Cyber Essesntials Plus, a certification which gives you peace of mind that your defences will protect against the vast majority of common cyber-attacks.

FULL SECURITY TESTING

Penetration testing, also called pen testing or ethical hacking, is the practise of testing a computer system, network or web application to find security vulnerabilities, that an attacker could exploit. Penetration tests assess your system for potential weaknesses that could result from poor or improper configuration, known and unknown hardware or software flaws. An experienced penetration tester will mimic the techniques used by criminals without causing damage, enabling you to address the security flaws that leave your organisation vulnerable.

BEST CYBER SECURITY OUTCOMES

Reduce the chances of security breaches

Maintain **confidentiality of** information

Minimise IT risks, possible damage and consequential costs

Increase trust with respect to partners, customers and the public

Obtain a competitive edge

Attract new business with the promise you have cyber security measure in place

Obtain a clear picture of your organisations cyber security

Follow a simple, straight forward process

Be listed on the directory of organisation's **awarded certification**

Increase your team's productivity

HOW CAN inTEC BUSINESS HELP WITH YOUR CYBER SECURITY AUDIT?

For complete peace of mind, protect your organisation's data, assets, and reputation with inTEC.

After contacting us, we'll be in touch as soon as possible to arrange an inTEC Security Audit. After completion, you'll receive a really useful report of your IT security capabilities and vulnerabilities along with a tailored list of recommendations of how you could improve your security. If you wish to move forward with any of the suggestions, we can make them happen.

Please contact us if you would like to discuss either continuing or starting your cyber security audit.

inTEC BUSINESS

0345 565 1767
info@intecbusiness.co.uk
intecbusiness.co.uk