Factory Internet
Cloud :: Connect :: Consult

Top Cyber Security Tips for SMEs

1. USE WHAT YOU ALREADY HAVE

A good place to start for any size business is to review the cyber protection already included in your existing subscriptions, such as Microsoft 365, antivirus, Router firewalls, cloud backups, email filtering and multi-factor authentication. Check that each feature is available, correctly configured, switched on and actively monitored before investing in additional security tools.

- **Switch on multi-factor authentication (MFA)** for email, cloud services, banking and admin accounts.
- **Use strong, unique passwords** and store them in a reputable password manager.
- **Enable automatic updates** for computers, phones, applications, browsers and network equipment.
- **Check antivirus is active**. Basic Microsoft Defender Antivirus is built into supported Windows systems.
- **Turn on email filtering** and strengthen Microsoft 365 or Google Workspace security settings.
- **Remove unused accounts and software** so attackers have fewer opportunities.
- **Administrator access** should be restricted.
- **Back up important information** automatically and test that it can be restored.
- **Train employees** to recognise attacks and give them a simple way to report suspicious emails or activity.
- **Configure your router firewall** settings for things like Restricting selected sites and services, Allowing specific connected devices & guest Wi-Fi isolation to separate visitors from business.

Ready to strengthen your cyber security?

Contact us today!

01424 540 175

sales@factoryinternet.co.uk

www.factoryinternet.co.uk

Factory Internet
Cloud :: Connect :: Consult

2. WORK TOWARDS CYBER ESSENTIALS

Cyber Essentials helps formalise the basics, reduce exposure to common attacks and demonstrate good practice to customers, insurers and supply-chain partners. Cyber Essentials Plus adds independent technical verification to those controls.

Cyber Essentials focuses on **five fundamental controls:**

SECURITY UPDATES

ACCESS CONTROL

FIREWALLS & ROUTERS

MALWARE PROTECTION

SECURE CONFIGURATION

Cyber Essentials is a cost-effective way to strengthen your business against common cyberattacks, starts at only a few hundred pounds and for eligible UK organisations, includes benefits such as cyber liability insurance.

3. IDENTIFY THINGS BEFORE CRIMINALS DO

Whilst Cyber Essentials demonstrates you take cyber security seriously as a business, it's not proof that every cyber risk is covered.

Over and above CE, regular vulnerability scanning continuously identifies new weaknesses, missing updates and configuration errors across your systems.

Penetration testing goes further by safely testing whether those weaknesses can be exploited. Together, they provide an ongoing view of your security posture. This will help you maintain your controls & security as threats and errors can change over time.

It will then allow you to prioritise findings by business risk, rather than treating every vulnerability as equally urgent. If you are confident in your set up, then Cyber Essentials Plus adds independent technical verification of the controls you've put in place.

Ready to strengthen your cyber security?

Contact us today!

01424 540 175

sales@factoryinternet.co.uk

www.factoryinternet.co.uk

4. IMPROVE DETECTION & RESPONSE

If your business is growing, then you might have to answer questions such as whether you are holding sensitive customer data, you facing contract, regulatory or insurance requirements, or whether your business tolerate prolonged downtime. If you do, then you might need to consider some of the following methods additional detection & response:

- Centrally managed endpoint protection or EDR.
- Mobile-device and laptop management.
- Email-domain protection, including SPF, DKIM and DMARC.
- Cloud and identity monitoring.
- Centralised logging.
- A documented and tested incident-response plan.
- Regular access reviews and removal of unnecessary privileges.

5. FOR CONTINUOUS OVERSIGHT USE A MANAGED SOC

A Security Operations Centre (SOC) is a team of cyber security specialists, supported by monitoring technology, that watches over a business's devices, networks, cloud services and user accounts. It will detect suspicious activity, investigate threats and coordinate a rapid response, before an attack causes serious harm to your business.

A managed Security Operations Centre can provide:

- 24/7 monitoring and threat detection.
- Central visibility across devices, networks, cloud and identities.
- Expert investigation of suspicious activity.
- Rapid containment and incident escalation.
- Proactive threat hunting.
- Vulnerability management and remediation tracking.
- Compliance, insurer and customer reporting.

NEED SOME HELP?

Get in touch if you think you might need to talk through where your business is at, where it's headed & what we can recommend you sensibly & affordably put in place relative to your business goals. We provide **FREE 30 MINUTE CONSULTATIONS.**

Ready to strengthen your cyber security?

Contact us today!

01424 540 175

sales@factoryinternet.co.uk

www.factoryinternet.co.uk