Cyber Security Checklist
For Small Businesses

How to Use This Checklist

Print this out, tick off what you've done, and use the rest as your action list.

Network Security

- ☐ Firewall installed and regularly updated
- ☐ Intrusion Detection/Prevention System in place
- ☐ Network segmented (e.g. guest vs. internal)
- ☐ Secure VPN for remote access Zero Trust access model adopted

Data Protection & Backup

- ☐ Sensitive data is encrypted (at rest & in transit)
- ☐ Unnecessary data is securely deleted
- ☐ Regular backups in place (cloud & local)
- ☐ Backups are tested regularly
- ☐ Data Loss Prevention (DLP) tools in use

Access Management

- ☐ Least Privilege enforced across users
- ☐ Role-Based Access Control (RBAC) implemented
- ☐ Strong password policy in place
- ☐ Password manager provided to staff
- ☐ Multi-Factor Authentication (MFA) enabled on all key systems

Endpoint & Device Security

- ☐ Antivirus/endpoint protection on all devices
- ☐ Mobile Device Management (MDM) active
- ☐ Remote wipe enabled for lost/stolen devices
- ☐ Software and operating systems kept fully up to date

Tech Top Tip:

Don't reuse passwords

It's tempting, but it's also one of the fastest ways for hackers to jump from one account to another.

Security Policies & Awareness

- ☐ Staff receive regular cybersecurity training
- ☐ Clear internal security policies published and accessible
- ☐ Employees know how to report security incidents

Email, Web & App Protection

- ☐ Email filtering and anti-phishing measures in place
- ☐ Web content filtering enabled
- ☐ Only approved apps can be installed (application control)

Incident Reponse & Business Continuity

- ☐ Written Incident Reponse Plan created and shared
- ☐ Business Continuity Plan in place
- ☐ Offline access to key recovery steps and contacts

Audits, Testing & Compliance

- ☐ Regular internal audits and vulnerability scans scheduled
- ☐ Penetration testing carried out annually
- ☐ Regulatory compliance (e.g. GDPR, Cyber Essentials) reviewed
- ☐ Vendor security practices checked

Physical Security

- ☐ Key hardware stored in locked/server-secure environments
- ☐ Visitor access controls and logging in place
- ☐ Surveillance and alarm systems used where appropriate

Reporting & Communication

- ☐ Staff know how and where to report suspicious activity
- ☐ Communication plan for internal/external staheolders exist
- ☐ ICO (or other regulators) contact process in place

www.zooc.co.uk

Still Unsure If You Have Everything Covered?

Even with a checklist, it can be hard to know if your business is fully protected. If you'd like peace of mind, get in touch with our team.