CORE NETWORK SOLUTIONS

Cybersecurity essentials checklist

The controls every organization should have in place

Most attacks use the same few ways in: stolen passwords, unpatched systems, phishing and weak backups. This checklist covers the basics that close those doors. Cyber insurers ask about many of them too.

Accounts and access

- [ ] Multi-factor authentication is on for email, remote access and every administrator account.
- [ ] Each person has their own account; no shared logins.
- [ ] Administrator rights are limited to the people who need them, and used only when needed.
- [ ] Accounts are removed promptly when people leave.

Devices and software

- [ ] Operating systems and applications are patched on a schedule.
- [ ] Every computer and server has endpoint protection that someone monitors.
- [ ] Laptops are encrypted.
- [ ] Unsupported software and devices have been replaced or isolated.

Email and people

- [ ] Email filtering blocks spam, malware and malicious links.
- [ ] Staff receive regular security awareness training.
- [ ] Staff know how to report a suspicious email, and are thanked for doing it.
- [ ] Payment changes and urgent money requests are always confirmed by phone.

Network

- [ ] A supported firewall protects every site, with rules reviewed at least yearly.
- [ ] Guest and business networks are separate.
- [ ] Remote access is through a VPN or zero-trust service with multi-factor authentication.

Backup and recovery

- [ ] Important data, including Microsoft 365, is backed up.
- [ ] At least one backup copy is off site, and can't be changed or deleted by an attacker.
- [ ] Restores are tested regularly.

Plan and test

- [ ] We have a written incident response plan, and know who to call.
- [ ] Our security is tested regularly, for example with a penetration test.
- [ ] Someone is responsible for security, and reports on it to management.

> **Next step**
>
> Every "no" is a gap worth closing. A security assessment gives you a clear picture and a practical plan, in order of priority.