



Cybersecurity Checklist

Protect your business from everyday cyber risks — one step at a time.

1. Strengthen Access Controls

- ☐ All employees use strong, unique passwords for every account
- ☐ Passwords are updated at least every 90 days
- ☐ Multi-factor authentication (MFA) is enabled for email, banking, and cloud tools

2. Keep Systems Up to Date

- ☐ All computers, mobile devices, and servers have automatic updates turned on
- ☐ Software and plugins are regularly reviewed for outdated versions
- ☐ Old or unsupported hardware has been retired or replaced

3. Back Up and Secure Data

- ☐ Daily or weekly backups are stored in two locations — one cloud, one offline
- ☐ Backup access is restricted and encrypted
- ☐ Backups are tested monthly to ensure files restore properly

4. Defend Against Email & Web Threats

- ☐ Employees are trained to spot phishing emails
- ☐ Spam filters and firewalls are active and maintained
- ☐ Suspicious links or attachments are never opened without verification

5. Train and Empower Your Team

- ☐ New-hire onboarding includes a quick cybersecurity orientation
- ☐ Quarterly refresher training reinforces awareness
- ☐ A clear incident response plan is in place (who to call, what to do)

6. Prepare for the Unexpected

- ☐ Insurance coverage includes cyber liability protection
- ☐ You have a trusted IT partner who monitors your systems 24/7
- ☐ Emergency contacts for your IT provider and backup providers are up to date

