

CYBER SECURE READY CHECKLIST

A practical guide to build resilience before the breach.

CYBER READY

You don't need a full-time IT department to take cyber readiness seriously. You just need ownership, consistency, and clarity on the basics. Use this checklist to prepare your business for stronger security—and faster recovery when something goes wrong.

People & Roles

- 0 One person is clearly responsible for digital security—even part-time.
- 0 All team members use strong, unique passwords.
- 0 Two-factor authentication (2FA) is turned on for all business accounts.
- 0 Security is part of staff onboarding and refreshers—at least annually.
- 0 Employees know how to report suspicious activity—and that it's encouraged, not punished.

Permissions & Access

- 0 User roles are reviewed quarterly (especially admin privileges).
- 0 Old accounts (former employees, interns, vendors) are deactivated promptly.
- 0 Shared logins are eliminated or managed through secure tools.
- 0 You know who has access to financial, HR, and customer systems—and why.

Email & Domain

- 0 SPF, DKIM, and DMARC are configured and monitored (ask your domain provider if unsure).
- 0 No inbox has forwarding rules to unknown addresses.
- 0 A staff member or vendor can check for unauthorized app connections or filters.
- 0 Your domain hasn't been flagged or blacklisted (tools like MXToolbox can check this).

Systems & Tools

- 0 A list of critical platforms (CRM, payroll, shipping, etc.) is maintained and up to date.
- 0 Each tool is secured with individual logins and 2FA where possible.
- 0 You maintain admin access to all essential systems—no single point of failure.

Response Readiness

- 0 You know who to call (internal or external) if there's a breach.
- 0 You've created a short response plan: what to check, who to alert, who communicates externally.
- 0 Regular backups are enabled for email, files, and key systems.
- 0 A short list of key client and vendor contacts is stored securely offline.



***This isn't about being perfect—
it's about being prepared.***

***A breach is stressful. This list helps ensure
your team can respond with clarity, not
chaos.***