FREE CYBER CHECKLIST

30-Point Small Business Cyber Risk Checklist

A practical checklist for finding common security gaps around accounts, MFA, email, AI tools, backups, vendors, and incident readiness.

Practical security organization guidance. Not legal, insurance, or compliance advice.

> This is not a full audit. Use it to find the obvious gaps first, then prioritize the highest-risk items.

1 Accounts And Access

- [ ] Every important account uses a unique password.
- [ ] Multi-factor authentication is enabled on email accounts.
- [ ] Multi-factor authentication is enabled on banking and payment tools.
- [ ] Multi-factor authentication is enabled on domain, hosting, and website accounts.
- [ ] Former employees, contractors, and vendors no longer have access.
- [ ] Admin accounts, including Microsoft 365 admin accounts, are limited to people who actually need them.

2 Devices

- [ ] Business laptops and desktops require a password or biometric login.
- [ ] Operating systems are set to update automatically.
- [ ] Antivirus or endpoint protection is active.
- [ ] Lost or stolen devices can be locked or wiped.
- [ ] Personal and business device use is clearly separated where possible.

3 Email And Phishing

- [ ] Employees know how to report suspicious emails.
- [ ] Payment-change requests require a second confirmation channel.
- [ ] Wire transfer or invoice changes are verified by phone or known contact.
- [ ] Email forwarding rules are reviewed for suspicious entries.
- [ ] The business has SPF, DKIM, and DMARC configured for its domain.

4 Data And Backups

- [ ] Critical files are backed up.
- [ ] Backups are tested at least quarterly.
- [ ] Sensitive client or customer data is stored only where needed.
- [ ] Shared folders are reviewed for excessive access.
- [ ] Important business data is not stored only on one laptop.

5 AI Tool Use

- [ ] Employees know not to paste passwords, API keys, customer data, financial records, legal documents, or confidential client work into public AI tools unless the business has approved the tool and data handling.

6 Vendors And Incident Readiness

- [ ] A list exists of key software vendors and SaaS tools.
- [ ] Critical vendors have known owners inside the business.
- [ ] Vendor admin accounts use multi-factor authentication.
- [ ] The business knows who to contact if a vendor account is compromised.
- [ ] The business has a simple incident contact list.
- [ ] Employees know who to call if something looks wrong.
- [ ] There is a written first-24-hours incident response checklist.
- [ ] Cyber insurance contacts, IT support, legal, and banking contacts are documented.

Your Score

0–12	High risk. Start with email, MFA, backups, admin access, and AI data handling.
13–24	Moderate risk. Clean up vendors, documentation, AI tool rules, and incident readiness.
25–30	Better than most small businesses. Review quarterly.

WHAT'S NEXT

Whether you prefer to do it yourself or work with an expert, the goal is the same: reduce your cyber risk before it becomes a business problem.

DIY PATH

Want the expanded tracker, policy templates, vendor inventory, backup checklist, and first-24-hours incident response worksheet?

Get the Starter Kit →

DONE-WITH-YOU PATH

Prefer an expert to review this with you and fix the highest-risk items directly?

Book a 30-Point Cyber Risk Assessment →