

The Small Business Cybersecurity Checklist

22 checks you can work through in an afternoon. Tick what is already true, and pick one unchecked item to fix this week.

Accounts and passwords

- ☐ Multifactor authentication is on for email, banking, payroll, and accounting.
- ☐ Every person has their own login; no shared passwords.
- ☐ A password manager is used instead of reused or written-down passwords.
- ☐ Former employees' accounts are closed the day they leave.

Email and payments

- ☐ Any change to payment details is confirmed by phone using a known number.
- ☐ Large or unusual payments need a second person's approval.
- ☐ Staff know how to report a suspicious email, and are thanked for doing it.

Devices and software

- ☐ Automatic updates are on for computers, phones, and the router.
- ☐ Laptops and phones have a screen lock and disk encryption turned on.
- ☐ Built-in or reputable security software is running on every computer.

Backups

- ☐ Important files are backed up automatically.
- ☐ At least one backup is kept offline or separate from your main accounts.
- ☐ You have tested restoring a file from backup in the last six months.

Customer data

- ☐ You know what customer, payment, and employee data you hold and where it lives.
- ☐ You keep only what you need, and securely delete the rest.
- ☐ Vendors that handle your data have been asked how they protect it.

AI tools

- ☐ You have a short list of approved AI tools on business accounts.
- ☐ Customer and employee details never go into unapproved tools.
- ☐ A person reviews AI-written content before it reaches a customer.

If something goes wrong

- ☐ You know who to call first: your bank, your IT help, and your insurer.
- ☐ You have written down where to report fraud (ic3.gov) and identity theft (identitytheft.gov).
- ☐ Someone knows how to check whether you must notify affected customers.