

Is your business secure and AI-ready?

A **5-minute self-assessment** for growing businesses. Tick every box that's true today, then add up your checks and see your score on the next page. **Every empty box is a gap**, and most are faster and cheaper to fix than you'd think.

1 • AI GUARDRAILS

- ☐ We have a simple, written rule for what staff can and can't put into AI tools
- ☐ Employees know never to paste client data, passwords, or secrets into public AI
- ☐ We've approved specific AI tools and discourage the rest
- ☐ Someone reviews new AI tools before the team starts using them

2 • PASSWORDS & ACCESS

- ☐ Everyone uses a password manager (no reused or sticky-note passwords)
- ☐ Multi-factor authentication (MFA) is on for email and key apps
- ☐ People can only access the systems they actually need
- ☐ Accounts are shut off the same day someone leaves

3 • YOUR HUMAN FIREWALL

- ☐ We run simulated phishing tests a few times a year
- ☐ Staff get security-awareness training more than once a year
- ☐ There's an easy, blame-free way to report a suspicious email
- ☐ New hires get security basics during onboarding

4 • DATA PROTECTION & BACKUPS

- ☐ Critical data is backed up automatically
- ☐ We've actually tested that a backup can be restored
- ☐ Sensitive files are encrypted
- ☐ We know where our most sensitive data lives

5 • COMPLIANCE & CYBER INSURANCE

- ☐ We carry cyber insurance
- ☐ We can meet the security controls our policy requires
- ☐ We can answer a client's security questionnaire without panic
- ☐ We follow (or are working toward) NIST CSF or CIS

6 • INCIDENT READINESS

- ☐ We have a written plan for "what if we get hacked"
- ☐ Everyone knows who to call first
- ☐ We've practiced it (even a quick tabletop) in the last year
- ☐ We know our notification obligations if data is exposed

STEP 1, SCORE YOURSELF

Add up your checked boxes (out of 24)

20–24 · Strong

You're ahead of most. Validate annually and close the last gaps.

13–19 · Exposed

Real gaps a determined attacker could use. Prioritize the empty boxes.

0–12 · High risk

You're one mistake from a costly incident. Fix the basics fast.

STEP 2, YOUR 5 FASTEST WINS

Do these this week

- 1 **Turn on MFA everywhere it's offered**
The single biggest risk reducer, most account breaches die here.
- 2 **Write a one-page AI usage rule**
Tell your team what's safe to put into AI tools, and what's never okay.
- 3 **Run one phishing simulation**
See where you actually stand before an attacker does.
- 4 **Test-restore a backup**
A backup you've never restored isn't really a backup.
- 5 **Check your cyber-insurance controls**
Pull the policy and confirm you meet what it requires, before you need to claim.

Counted more empty boxes than you'd like?

You don't need a full security team to close the gaps. Book a free, no-pressure call and we'll map your biggest risks and the fastest fixes, including safe AI adoption.