SECURITY BASICS, ONE BOX AT A TIME.

A checklist for an office that doesn't have a security department. Tick what's true today. What's left is your to-do list, in plain English.

COMPANY _____ FILLED IN BY _____ DATE _____

Tick a box only if you could show someone it's true. The list is sorted into the same eight areas our Cyber Readiness score uses. It isn't that score, and a full sheet of ticks isn't a certificate.

IDENTITY

Sign-in protection, admin accounts, and accounts that should have been closed.

- [ ] **Multi-factor sign-in is on for email.** Then for banking, payroll, and every other account that offers it.
- [ ] **Nobody shares a sign-in.** One person, one account, so you can see who did what and close one without breaking another.
- [ ] **Passwords live in a password manager.** Long, different for every site, and not in a spreadsheet or on a sticky note.
- [ ] **Admin accounts are kept for admin work.** People do their daily work in an ordinary account, and you can name everyone who holds an admin one.
- [ ] **A leaver's accounts are closed the day they leave.** The first day, last day checklist has the full list.

DEVICES

Whether every computer is protected and up to date.

- [ ] **You have a list of every computer.** Who uses it, and roughly how old it is.
- [ ] **Updates install without anyone having to remember.** The operating system, the browser, and the apps people use every day.
- [ ] **Nothing runs software its maker has stopped updating.** That includes the old PC in the back that runs one program.
- [ ] **Laptop disks are encrypted.** So a laptop left in a car doesn't hand over what's on it.
- [ ] **Antivirus is on, up to date, and reporting to someone.** A warning nobody sees isn't protection.
- [ ] **Screens lock when people walk away.** And any phone that gets work email has a passcode.

EMAIL AND APPS

How your email and your cloud apps are locked down.

- [ ] **Everyone knows the signs of a phishing email.** Four signs an email is working on you is a good place to start.
- [ ] **A change to payment details is always confirmed by phone.** Using a number you already had, not the one in the email.
- [ ] **No mailbox forwards mail outside the company unless you meant it to.** A forwarding rule nobody remembers setting is worth a hard look.

- [ ] **You know which cloud apps hold company data.** And who the admin is for each one.
- [ ] **Apps connected to mailboxes and files have been reviewed.** If nobody uses one any more, disconnect it.
- [ ] **Your email domain has SPF, DKIM, and DMARC set up.** They make it harder to send fake mail in your name. Whoever looks after your email can tell you.

BACKUP

What's backed up, and whether a restore has been tested.

- [ ] **The data you can't lose is backed up.** Including what lives in Microsoft 365 or Google Workspace.
- [ ] **One copy is somewhere an attacker can't reach.** Away from the office, and locked against being changed or deleted.
- [ ] **Someone has restored a file from it lately.** As a test, not in an emergency.
- [ ] **A backup that fails tells a person.** And that person does something about it.
- [ ] **You've asked the harder questions.** The backup checklist has them.

NETWORK

The edge of your network, and how current its rules are.

- [ ] **The router and the firewall aren't on the password they came with.** And the new one is in the password manager.
- [ ] **Network equipment gets updates too.** The router, the firewall, and the Wi-Fi, not only the computers.
- [ ] **Guests get their own Wi-Fi.** Visitors and personal devices stay off the network your work is on.
- [ ] **Nothing in the office is open straight to the internet.** Remote access goes through a VPN or a managed remote tool, with multi-factor sign-in.
- [ ] **The Wi-Fi password changes when someone who knew it leaves.** Better still, each person signs in to Wi-Fi as themselves.

DETECTION AND RESPONSE

Whether trouble would be noticed, and how ready the response is.

- [ ] **Alerts go to a person who acts on them.** Antivirus warnings, sign-in warnings, and failed backups.
- [ ] **Sign-in alerts are switched on.** For email, and for every admin account.
- [ ] **Staff know who to tell.** One name and one number, and no blame for owning up to a click.
- [ ] **Activity logs are kept.** Long enough to look back once you find out something went wrong.

PEOPLE

Security training, how people are keeping up with it, and cover for key people.

- [ ] **Everyone gets security training.** Short and regular sticks. Long and once doesn't.
- [ ] **New starters get it early.** Before the first fake invoice lands in their inbox.

- [ ] **People know the rules for AI tools.** What may go into a chatbot, and what never does. The AI policy template is a start.
- [ ] **No critical job depends on one person being in.** Banking, payroll, and the admin sign-ins each have a second person who can step in.

PLAN MATURITY

Written, signed plans for staying open and for handling an incident.

- [ ] **There's a written plan for a bad day.** Who decides, who calls whom, and what gets switched off.
- [ ] **The important phone numbers are on paper.** IT, the bank, the insurer, and a lawyer. A contact list in email is no use when email is down.
- [ ] **The plan has been practised.** Talk one made-up incident through around a table.
- [ ] **You know what your insurer and your customers expect of you.** Any security terms in a policy or a contract are written down where you can find them.
- [ ] **The plan has an owner.** Someone rereads it after any big change.