

The Complete Small Business Cybersecurity Checklist 2026

Print this. Tick what you do. Circle three gaps for this month. Educational guidance by James Lugton, Cyber Security Analyst — not formal assurance.

1. Identity & access

- Own logins — no shared banking password
- Password manager for money / email / admin
- MFA on email, banking, accounting, workspace, website admin
- Leavers lose access the same day
- Admin rights limited on PCs

2. Devices & updates

- Screen locks + current OS
- Auto-updates on; monthly router check
- Lost/stolen process written down
- BYOD follows MFA/update rules

3. Email, invoices & money

- Verify bank-detail changes out-of-band
- New payee / changed IBAN = pause and confirm
- Second pair of eyes above a threshold
- Blame-free phishing reporting

4. Backups

- Backups separate from live machine
- Restore tested in last 12 months
- Not only an always-connected copy

5. Website, payments & data

- Plugins/themes updated
- Admin MFA where offered
- Know PCI SAQ type if taking cards
- No customer data on random USBs

6. People

- 30-minute starter briefing
- Quarterly real-example huddle
- No customer data in public AI bots
- One-page if-wrong card

7. When things go wrong

- Who decides offline / customer / bank
- Break-glass admin offline
- Action Fraud / ICO / insurer notes

90-day starter: 1–30 MFA + password manager + leaver checklist. 31–60 backup test + invoice rule + updates. 61–90 staff huddle + AI rules + website tidy.

