



Master SMB Cybersecurity Audit Checklist

25-Point Small Business Cyber Readiness Audit

- Are critical accounts inventoried?
- Is MFA enabled everywhere important?
- Are passwords unique?
- Are dormant users removed?
- Is website software updated?
- Is domain registrar MFA enabled?
- Is hosting access reviewed?
- Is business email MFA enabled?
- Are fake invoice scams discussed?
- Are payment changes voice-verified?
- Are employee laptops reviewed?
- Are business phones considered secure endpoints?
- Are software updates enforced?
- Are backups automated?
- Has restore been tested?
- Are backups isolated?
- Are suspicious login alerts enabled?
- Is website uptime/SSL monitored?
- Are strange inbox events monitored?
- Do employees report suspicious messages?
- Is customer payment trust protected?
- Is monthly cyber review assigned?
- Is vendor access reviewed?
- Is a simple cyber checklist documented?
- Would a moderate cyber incident be manageable tomorrow?

Scoring:

21–25 = Strong SMB cyber maturity

15–20 = Moderate operational exposure

0–14 = High avoidable cyber vulnerability