Small Business Cybersecurity Checklist

Checklist · For Solo Operators And SMBs (1-25 Employees) Without IT.

Most SMB breaches are preventable with five baseline controls. This checklist gets you to a defensible security posture without hiring a full-time IT person.

Identity & Access

- Every employee has their own login — NO shared passwords.
- Business password manager deployed (1Password Business, Bitwarden Business).
- MFA required on email, accounting, payroll, banking, and admin tools — authenticator app preferred.
- Onboarding/offboarding checklist includes account creation/disabling.
- Admin accounts separated from daily-use accounts.
- Quarterly review of who has access to what — remove unused accounts.

Endpoint Security

- Every company device has full-disk encryption (FileVault / BitLocker).
- Endpoint protection running (Defender for Windows, plus Malwarebytes Premium or similar).
- Auto-updates ON for OS, browsers, productivity software.
- Mobile device management (MDM) for company phones if applicable (Microsoft Intune, Jamf).
- Personal-device policy documented if employees use their own laptops.

Email & Phishing Defence

- Business email uses SPF, DKIM, and DMARC records.
- External email warnings enabled (banner on inbound external mail).
- Anti-phishing training run at least annually (KnowBe4, Hoxhunt, or free PhishMe alternatives).
- Reporting button or shared mailbox for employees to flag suspicious email.
- Wire-transfer requests require out-of-band verification (callback to a known number).

Data & Backups

- Critical data backed up daily (automated, not manual).
- Backups follow 3-2-1 rule (3 copies, 2 media types, 1 offsite).
- Restore tested quarterly — not just the backup, the actual restore.
- Customer/client PII storage minimised — keep what you need, delete the rest.
- Encrypted-at-rest cloud storage for sensitive files.

Compliance & Insurance

- Industry-specific compliance reviewed (HIPAA, PCI-DSS, state privacy laws).
- Privacy policy on website is accurate and up to date.
- Cyber-liability insurance quote obtained — even basic coverage is worth it.
- Vendor risk: list of third parties that hold your data, with security review notes.
- Incident response plan written down (page 1: who to call when something happens).

Training & Culture

- All employees complete annual security awareness training.
- New hires get a security briefing in their first week.
- Acceptable use policy signed by every employee.
- Security incidents reviewed in monthly all-hands or team meetings.

SCAM ALERT

Toll-Road SMS Scam Is Spreading Across The U.S.

Texts claiming you owe a small toll fee link to fake DMV-style sites. They steal card numbers and SSNs. Never click a 'toll' link — go to the toll authority directly.

Visit Making Sense Of Security →