

Small Business Cybersecurity Checklist

Eleven practical controls for teams of roughly 5–100 people. Tick each box when it's done, then revisit the list every quarter. From Small Biz Cyber Guide (smallbizcyberguide.com).

- | | |
|-----|---|
| [] | 1. Turn on MFA everywhere
Email, banking, payroll, cloud admin and remote access first. Prefer authenticator apps or passkeys over SMS codes.
Guide: MFA for Microsoft 365 |
| [] | 2. Use a team password manager
Unique passwords for every account, shared vaults instead of spreadsheets, and an offboarding plan for departing staff.
Guide: Password managers for small business |
| [] | 3. Back up and test restores
Follow 3-2-1: three copies, two media types, one offsite or immutable. Test a restore at least quarterly. Cloud sync is not a backup.
Guide: Backup for freelancers and SMBs |
| [] | 4. Keep everything updated
Turn on automatic updates for operating systems, browsers and apps. Replace devices that no longer get security patches.
Guide: Automatic updates for small business |
| [] | 5. Lock down email: SPF, DKIM, DMARC
Publish SPF and DKIM for every service that sends mail as you, then move DMARC from p=none toward quarantine or reject.
Guide: SPF, DKIM and DMARC guide |
| [] | 6. Train for phishing and quishing
Teach staff to verify payment or password requests by phone, and to treat QR codes in emails, flyers and parking signs as links.
Guide: QR code phishing (quishing) |
| [] | 7. Secure remote access with a business VPN
Avoid exposing RDP or admin panels to the internet. Use a business VPN or zero-trust access with MFA for remote staff.
Guide: Business VPN for remote teams |
| [] | 8. Offboard the same day
Disable email and cloud accounts, remove the person from the password vault, rotate shared logins, and collect devices when someone leaves.
Guide: Employee offboarding checklist |
| [] | 9. Verify payments by callback
For wire, ACH, or bank-detail changes, call a known number from your records - never the number in the email - before paying.
Guide: Spot the fake wire request |

[] **10. Encrypt every laptop disk**

Turn on BitLocker (Windows) or FileVault (Mac), store recovery keys in your password manager, and verify encryption on every company laptop.

Guide: [Disk encryption for every laptop](#)

[] **11. Protect every endpoint**

Run managed endpoint protection (EDR where possible), enable disk encryption, and keep a list of every company laptop and phone.

Guide: [Endpoint protection for small business](#)

Need a professional security test? Northline Digital offers SMB-focused penetration testing and security reviews: northlinesec.com.

Some guides on smallbizcyberguide.com contain labeled affiliate links; see smallbizcyberguide.com/affiliate-disclosure. © 2026 Northline Digital LLC.