Synergy Technology Managed IT

Small Business Cybersecurity Checklist

Tampa, FL | synergytek.net

Protect your business in 30 minutes or less

Use this checklist to audit your current security posture. Check off each item you have in place. Any unchecked item is a potential vulnerability — reach out to us for help closing the gaps.

■ Passwords & Authentication

- ■ All accounts use unique, complex passwords (12+ characters)
  Tip: Use a password manager — Bitwarden is free, 1Password is excellent for teams.
- ■ Multi-factor authentication (MFA) enabled on email accounts
  Priority: Microsoft 365 and Google Workspace first.
- ■ MFA enabled on banking, payroll, and financial platforms
- ■ MFA enabled on remote access tools (VPN, RDP, remote desktop)
- ■ Default passwords changed on all routers, switches, and devices
  Factory default passwords are publicly searchable — change them immediately.
- ■ Password manager deployed for all staff

■■ Endpoint & Device Security

- ■ Antivirus/EDR software installed and active on all workstations
  EDR (Endpoint Detection & Response) is significantly more effective than basic antivirus.
- ■ Operating systems set to auto-update on all devices
- ■ All third-party software (browsers, Adobe, Java) kept up to date
  60% of breaches exploit known vulnerabilities with patches already available.
- ■ Full-disk encryption enabled (BitLocker on Windows, FileVault on Mac)
  Critical for laptops — if stolen, data is unreadable without the key.
- ■ Screen lock set to activate after 5 minutes of inactivity
- ■ Mobile devices enrolled in MDM (mobile device management)

■ Email & Phishing Protection

- ■ Email filtering / spam protection enabled (built-in or third-party)
- ■ SPF, DKIM, and DMARC records configured for your domain
  These prevent criminals from spoofing your email domain to scam your clients.
- ■ Staff trained to recognize phishing emails in the past 12 months
  Even 1 hour of awareness training dramatically reduces click rates.
- ■ Process in place to report suspicious emails to IT
- ■ Email archiving enabled for compliance and recovery

■ Backup & Disaster Recovery

- ■ Business data backed up daily (at minimum)
- ■ Backups follow the 3-2-1 rule: 3 copies, 2 media types, 1 offsite/cloud
  Backups on the same network as production data can be wiped by ransomware.
- ■ Backup restore has been tested in the past month
  Untested backups fail when you need them most — monthly testing keeps you ready.
- ■ Cloud data (Microsoft 365, Google Workspace) separately backed up
  Cloud providers are NOT responsible for backing up your data — you are.
- ■ Recovery time objective (RTO) documented: how long can you be down?

☐ Network & Access Control

- ☐ Guest Wi-Fi network separate from business network
- ☐ Firewall active and configured on business router
- ☐ VPN required for remote employees accessing internal systems
- ☐ Admin accounts separate from daily-use accounts

Never browse the web or check email logged in as an administrator.

- ☐ Former employee access revoked same day they leave

Access reviews should happen quarterly — not just at offboarding.

- ☐ Least-privilege access: employees only access what they need

☐ Policies & Compliance

- ☐ Acceptable use policy documented and signed by all staff
- ☐ Incident response plan exists (what to do if you get breached)

Having a plan reduces breach costs by an average of $2.6M per IBM.

- ☐ Cyber liability insurance policy in place and reviewed annually
- ☐ Vendor/third-party access reviewed and limited
- ☐ Annual security review scheduled with your IT provider

Your Security Score Items checked: ___ / 32 *0–15: High Risk | 16–24: Moderate | 25–32: Strong*