

# The SMB Cybersecurity Checklist

25 controls every small and midsize business should have in place. Check off what you have. Every blank box is a gap an attacker can use.

## Identity & access

---

- ☐ Multi-factor authentication (MFA) is on for email, VPN, remote access, and every admin account.
- ☐ Every employee has their own login. No shared accounts or shared passwords.
- ☐ A password manager is used company-wide, and passwords are never reused.
- ☐ Departing employees lose access the same day they leave.
- ☐ Admin rights are limited to the few people who truly need them.

## Devices & network

---

- ☐ Every computer runs managed endpoint protection (EDR), not just free antivirus.
- ☐ Operating systems and apps are patched automatically, and you can prove it.
- ☐ Laptops are encrypted (BitLocker or FileVault).
- ☐ The firewall is business-grade, with firmware that's up to date and still supported.
- ☐ Guest Wi-Fi is separated from the business network.
- ☐ You have a current list of every device and who uses it.

## Email & people

---

- ☐ Email filtering blocks phishing, malicious links, and dangerous attachments.
- ☐ SPF, DKIM, and DMARC are set up for your domain.
- ☐ Staff complete security awareness training at least twice a year.

- ☐ Wire transfers and payment changes need verbal confirmation using a known phone number.

## Backup & recovery

---

- ☐ Critical data is backed up daily, with at least one copy offline or immutable.
- ☐ Microsoft 365 or Google Workspace data is backed up separately. The provider's built-in retention isn't a backup.
- ☐ A full restore has been tested in the last 90 days.
- ☐ You know how many hours your business can stay down, and your backups meet that target.

## Monitoring & response

---

- ☐ Security alerts are watched 24/7 by a person or a service, not just logged.
- ☐ There's a written incident response plan that says who to call first.
- ☐ You have cyber insurance, and you meet its security requirements.
- ☐ Vendors and apps with access to your data are reviewed every year.
- ☐ Logs are kept long enough to investigate an incident (90 days or more).
- ☐ Someone owns cybersecurity, internally or through a partner, and reviews it quarterly.

### More than three blank boxes? Let's close them.

Book a **free 15-minute IT & security consult** with Ascent Strategies. We'll go through your results and point out the fixes that matter most, with no pressure and no jargon.

**[ascentstrateges.com/contact](https://ascentstrateges.com/contact) · 512-615-9255**