// FREE CHECKLIST

Small Business Cybersecurity Checklist

20 critical security controls every small business should have in place. Use this checklist to find your gaps — before attackers do.

60% **of small businesses that suffer a cyberattack close within 6 months.** Most were operating without the basic protections covered in this checklist.

01 ACCESS & PASSWORDS

- [ ] **All accounts use strong, unique passwords** — CRITICAL
  Minimum 12 characters, no reused passwords across accounts. Use a password manager like Bitwarden or 1Password.
- [ ] **Multi-factor authentication (MFA) is enabled** — CRITICAL
  Enabled on email, banking, cloud storage, and any remote access tools.
- [ ] **Admin accounts are separate from daily-use accounts** — HIGH
  Admin privileges should not be used for everyday tasks like browsing or email.
- [ ] **Former employee accounts are promptly deactivated** — HIGH
  Access should be revoked within 24 hours of an employee departure.

02 SOFTWARE & UPDATES

- [ ] **Operating systems are set to auto-update** — CRITICAL
  Windows, macOS, and mobile devices should install security patches automatically.
- [ ] **Antivirus / endpoint protection is installed and active** — CRITICAL
  All business devices should have active, updated endpoint protection software.
- [ ] **Business software is licensed and up to date** — HIGH
  Unlicensed or outdated software does not receive security patches.

- [ ] **Unused software and apps are removed** — MEDIUM
  Every installed application is a potential attack surface. Remove anything not actively used.

03 NETWORK & WI-FI

- [ ] **Business Wi-Fi uses WPA3 or WPA2 encryption** — CRITICAL
  Never use WEP or open networks for business operations.
- [ ] **Guest Wi-Fi is on a separate network from business systems** — HIGH
  Customers and visitors should never share a network with your business devices.
- [ ] **Router default passwords have been changed** — CRITICAL
  Default router credentials are publicly known and actively exploited.
- [ ] **Firewall is enabled on all devices and the router** — HIGH
  Both hardware (router) and software (device) firewalls should be active.

04 DATA & BACKUPS

- [ ] **Business data is backed up regularly (3-2-1 rule)** — CRITICAL
  3 copies, on 2 different media types, with 1 stored offsite or in the cloud.
- [ ] **Backups have been tested and verified restorable** — HIGH
  An untested backup is not a backup. Verify restoration at least quarterly.
- [ ] **Sensitive customer data is encrypted at rest** — HIGH
  Any stored PII, payment data, or health records should be encrypted.
- [ ] **A data retention and disposal policy exists** — MEDIUM
  Old data should be securely deleted — not just abandoned on old drives or cloud folders.

05 EMAIL & PHISHING

- [ ] **Staff have received phishing awareness training** — CRITICAL
  Phishing is the #1 entry point for attackers. All employees should know what to look for.
- [ ] **Email domain has SPF, DKIM, and DMARC records configured** — HIGH
  These DNS records prevent attackers from spoofing your business email domain.
- [ ] **There is a clear process for reporting suspicious emails** — MEDIUM
  Employees should know exactly who to contact if they suspect a phishing attempt.
- [ ] **Business email is hosted on a professional platform** — MEDIUM
  Avoid personal Gmail/Yahoo for business. Use Google Workspace, Microsoft 365, or similar.

// HOW TO SCORE YOUR RESULTS

0 – 7
High Risk

Significant gaps present. Immediate action recommended before an incident occurs.

8 – 14
Moderate Risk

Good start, but key vulnerabilities remain that could expose your business.

15 – 20
Strong Posture

Well protected. Focus on maintaining controls and testing them regularly.

Find out exactly where you stand.

Root Command IT offers free 30-minute security assessments for local small businesses. No sales pitch — just a clear picture of your risk and what to do about it.

ROOTCOMMANDIT.COM/CONTACT