✅ The Essential Cybersecurity Checklist for Small Business Owners

10 quick wins to protect your business, your data, and your reputation—no IT degree required.

Section 1: Quick Self-Assessment (Check all that apply)

☐ We require strong, unique passwords for all accounts

☐ Multifactor authentication (MFA) is enabled on email, file sharing, and critical apps

☐ Employees receive cybersecurity training at least twice a year

☐ Our systems and software are patched regularly (monthly or better)

☐ We use a business-grade antivirus or EDR solution

☐ We back up our data daily and test our backups monthly

☐ We have a plan for responding to a cyberattack or ransomware incident

☐ Only authorized staff have access to sensitive data (role-based access)

☐ We immediately revoke access for employees who leave the company

☐ Our team knows how to spot phishing emails and social engineering tactics

Score Yourself:

✅ 8–10 checks: You're in great shape!

⚠️ 5–7 checks: You're on the right path, but there are critical gaps to fix.

❌ 0–4 checks: You're at high risk—prioritize action now.

Section 2: The Top 5 Threats (With Fixes)

- **Phishing & Social Engineering**

Train employees regularly, simulate phishing attacks, and enable MFA.

- **Weak or Reused Passwords**

Use a password manager, enforce strong password policies, and enable MFA.

- **Unpatched Software**

Keep software up to date, automate patches, and retire unsupported tools.

- **Ransomware**

Back up data daily, use EDR tools, and test your recovery plan.

- **Insider Threats**

Use role-based access, monitor behavior, and educate staff on data handling.

Section 3: What to Do Next

• Schedule a Free Cybersecurity Consultation with our experts

• Get Our Full Cybersecurity Toolkit for SMBs

• Join our newsletter for monthly IT tips and security updates

• Visit www.frcstech.com to get started today.