



Small Business Cyber Security Checklist

12 Essential Security Measures for 2026 | bsg.tech

2025 Verizon DBIR Key Stats: Stolen credentials used in **33%** of SMB breaches. Ransomware present in **88%** of small business attacks (vs 39% for large orgs). MFA is your best defense.

Quick Wins (Start Here)

- Enable 2FA on all email and cloud accounts today
- Deploy a password manager company-wide
- Enable automatic updates on all devices
- Verify backup restoration works

1. Password Management

- ☐ **Deploy enterprise password manager** – 1Password, Bitwarden, or Apple Passwords for all employees
- ☐ **Enforce unique, random passwords** – Minimum 16 characters generated by password manager

2. Two-Factor Authentication (2FA)

- ☐ **Enable MFA on all business accounts** – Email, cloud storage, CRM, banking, social media
- ☐ **Use authenticator apps** – Google Authenticator, Authy, or password manager OTP (never SMS)
- ☐ **Deploy hardware keys for admins** – YubiKey for IT staff and privileged accounts
- ☐ **Adopt passkeys where available** – Passwordless future: Apple, Google, Microsoft support

3. Automatic Updates

- ☐ **Enable auto-updates on all systems** – Windows, macOS, Linux, mobile devices
- ☐ **Update business applications** – Browser, Office, Slack, Zoom, accounting software
- ☐ **Patch network devices** – Routers, firewalls, NAS devices, printers

4. Backup Strategy

- ☐ **Implement 3-2-1 backup rule** – 3 copies, 2 different media, 1 offsite/cloud
- ☐ **Encrypt all backup data** – Before uploading to cloud storage
- ☐ **Test restoration quarterly** – Verify you can actually recover from backups

5. Attack Surface Reduction

- ☐ **Run network discovery scans** – Use runZero for asset discovery and inventory
- ☐ **Close unnecessary ports** – Disable RDP, VNC, SSH if not needed publicly
- ☐ **Scan for vulnerabilities** – Nmap, Nuclei, or Nessus monthly

6. Web Application Protection

- ☐ **Deploy Cloudflare (free tier)** – WAF, DDoS protection, SSL for all websites
- ☐ **Restrict origin access** – Only allow connections from Cloudflare IPs
- ☐ **Enable HTTPS everywhere** – Force SSL/TLS on all web properties

7. Configuration Security

- ☐ **Audit Active Directory** – Run Ping Castle and fix critical findings
- ☐ **Audit cloud infrastructure** – Scout Suite for AWS/GCP/Azure
- ☐ **Review access permissions** – Remove ex-employees, limit admin accounts

8. Centralized Logging

- ☐ **Enable logging on all systems** – Windows Event Log, Linux syslog, cloud audit logs
- ☐ **Centralize log storage** – Loggly, Elastic Security, or cloud-native SIEM
- ☐ **Set up basic alerts** – Failed logins, admin changes, unusual access patterns

9. Threat Detection

- ☐ **Deploy canary tokens** – Free tripwires from canarytokens.org
- ☐ **Monitor for warning signs** – Failed logins, new accounts, disabled security
- ☐ **Have incident response plan** – Know who to call if breached

10. Endpoint Security

- ☐ **Enable built-in protection** – Windows Defender, macOS firewall enabled
- ☐ **Configure real-time scanning** – Antivirus with daily full scans
- ☐ **Enable disk encryption** – BitLocker (Windows), FileVault (macOS)

11. Security Testing

- ☐ **Create security.txt file** – Invite responsible disclosure on your website
- ☐ **Consider annual pentest** – Professional assessment of your security posture
- ☐ **Explore bug bounty** – HackerOne, BugCrowd for continuous testing

12. Ongoing Security Hygiene

- ☐ **Quarterly security review** – Check all items above, update as needed
- ☐ **Employee offboarding process** – Revoke access same-day for departures
- ☐ **Security awareness training** – Annual training for all employees

Free Tools Mentioned in This Checklist

- **Password managers:** Bitwarden (free tier), Apple Passwords (built-in)
- **2FA & Passkeys:** Google Authenticator, Authy, FIDO Alliance passkeys
- **Web protection:** Cloudflare (free tier)
- **Network discovery & scanning:** runZero, Nmap, Nuclei
- **Configuration audit:** Ping Castle, Scout Suite, Prowler
- **Threat detection:** canarytokens.org, Open Canary
- **Endpoint:** Windows Defender, OSQuery



Need help implementing this checklist?

BSG provides penetration testing, security assessments, and consulting for small businesses.

bsg.tech/contact | bsg.tech/penetration-testing

Download the full guide: bsg.tech/blog/small-business-cyber-security-checklist