SMB Shield Starter - 14-Day Quickstart Checklist

A practical, low-friction baseline for a small business to reduce ransomware and account-takeover risk fast - without buying new tools.

Target outcomes	What you need	What you get
• MFA everywhere • Recoverability in 24-72h • Fewer 'one-click' breaches	Admin access to Microsoft 365/Google + endpoints + router/firewall	A one-page score + evidence pack to prove baseline controls

14-Day plan (tick boxes)

When	Theme	Actions
Day 1-2	**Lock identities**	[] Turn on MFA for admins + all users [] Disable legacy auth / basic IMAP/POP where possible [] Create 2 break-glass accounts (MFA + stored offline)
Day 3-4	**Secure email**	[] Enable phishing protection + DMARC baseline [] Block auto-forwarding to external addresses [] Review risky mailbox rules
Day 5-6	**Backups you can restore**	[] Identify 3 critical systems (finance, CRM, file shares) [] Ensure at least 1 offline/immutable backup copy [] Verify restore access is separate from daily admin
Day 7-8	**Endpoint baseline**	[] Patch OS + browsers + PDF readers [] Enable full-disk encryption [] Remove local admin rights from daily accounts
Day 9-10	**Least privilege**	[] Separate admin accounts from daily accounts [] Audit vendor access (time-bound, MFA, named users) [] Turn on logging: sign-ins + admin actions
Day 11-12	**Ransomware containment**	[] Segment backups, NAS and admin tools from user network [] Block unsigned macros by default [] Confirm EDR/AV is active on all endpoints
Day 13	**Recovery drill**	[] Run a 60-minute restore drill: one laptop + one shared folder [] Document RTO/RPO (how fast, how much data loss)
Day 14	**Executive sign-off**	[] Create your 1-page baseline report + evidence links [] Assign owners + quarterly review cadence

Subscriber bonus: full templates pack + guided onboarding checklist (evidence-driven, audit-friendly).