Multi-Factor Authentication (MFA) Setup Checklist for Small Businesses (2026 Edition)

This checklist helps you implement MFA across your business, not just on one account, but everywhere it matters.

MFA Setup Checklist

1. Choose the Right MFA Method

□ Authenticator app is selected (recommended)
□ Passkeys are used where supported
□ Hardware security keys are considered for high-risk users
□ SMS is used only as a backup option

Why this matters:
Stronger MFA methods reduce the risk of interception or bypass.

2. Enable MFA on Business Email (Critical First Step)

□ Microsoft 365 MFA is enabled
□ Google Workspace MFA is enabled
□ All users are enrolled—not optional
□ Admin accounts are prioritized

Why this matters:
Email is the most common entry point for account compromise.

3. Secure Financial and Banking Accounts

□ MFA is enabled for banking platforms
□ Payment systems require verification
□ Access is limited to authorized personnel

Why this matters:
Financial accounts are high-value targets for attackers.

4. Enable MFA on Social Media and External Platforms

□ Facebook, Instagram, LinkedIn secured
□ Business accounts are protected
□ Admin access is limited and controlled

Why this matters:
Social platforms are often used for impersonation and fraud.

5. Protect Cloud Storage and Business Applications

□ Google Drive, OneDrive, Dropbox secured
□ SaaS applications require MFA
□ Shared platforms enforce access controls

Why this matters:
Cloud storage often contains sensitive business data.

6. Secure Your Password Manager

□ MFA is enabled on password manager
□ Device-based approval is configured
□ Access is restricted to authorized users

Why this matters:
Your password manager protects every other account, secure it first.

7. Secure Device-Level Access

□ Phones require biometric or PIN login
□ Computers require secure login
□ Apple, Google, or Microsoft accounts have MFA enabled

Why this matters:
MFA depends on trusted devices. If the device is compromised, access is at risk.

8. Store Backup Codes Securely

□ Backup codes are saved in a password manager
□ Printed copies are stored securely
□ Access to codes is limited

Why this matters:
Backup codes prevent lockouts if devices are lost.

9. Test MFA and Account Recovery

□ Users log out and log back in using MFA
□ Recovery process is verified
□ Issues are resolved before rollout

Why this matters:
Testing ensures MFA works when it's actually needed.

10. Maintain and Update MFA Settings

□ MFA is updated when devices change
□ Employee changes trigger access updates
□ Old devices and methods are removed

Why this matters:
Outdated MFA settings create security gaps over time.

What a Fully Secured MFA Environment Looks Like

Every critical account requires MFA
Strong authentication methods are used
Access is controlled and monitored
Recovery options are secure and tested

Quick Rule of Thumb

If MFA is not required everywhere, attackers will target the place it isn't.

SofTouchSystems.com

No-Surprise IT — Predictable. Proactive. Proven.