# MFA Comparison Chart + Setup Quick Guide

## Part 1: MFA Method Comparison

|  |  |  |  |
| --- | --- | --- | --- |
| MFA Method | Security Level | Ease of Use | Recommended For |
| Text Message (SMS) | Low | High | Only when no other option is available |
| Authenticator App (TOTP) | Medium-High | Medium | Most personal & business accounts |
| Push Notification App | High | High | Microsoft, Google, Duo users |
| Hardware Token (e.g., YubiKey) | Very High | Medium | High-risk users or admins |
| Biometrics (Face ID, Fingerprint) | High | Very High | Mobile devices & secured laptops |

## Part 2: Quick Setup Tips

Use these general steps to enable MFA on most accounts:

1. Log in to your account and find the Security or Account Settings section.

2. Look for an option to enable Multi-Factor or Two-Factor Authentication.

3. Choose your preferred method (authenticator app, hardware key, etc.).

4. Scan the QR code with your authenticator app or insert your hardware key.

5. Save your backup codes in a secure offline location.

6. Test your new login setup to ensure everything works properly.

✅ Bonus Tip: Register a second device or method for backup access if the service allows it.