Beginner's Guide To Two-Factor Authentication

Guide · Why MFA Matters, Which Method To Use, And How To Migrate Without Locking Yourself Out.

Who this is for: anyone who has heard 'enable 2FA' but isn't sure what it is, which kind to use, or how to set it up without breaking things. This guide explains the why, the hierarchy of methods, and the safe migration path.

Why MFA Matters

A password is one factor: something you know. MFA — Multi-Factor Authentication, also called 2FA (Two-Factor) — adds a second factor: something you have (a phone, a hardware key) or something you are (a fingerprint, face). Even if your password leaks in a breach, an attacker without your second factor can't log in. MFA is the single most effective defence against account takeover after using a password manager.

The MFA Hierarchy

Not all MFA methods are equally secure. Use the strongest available for each account:

Method	Security	How It Works	Use For
Hardware key (YubiKey, Titan)	★★★★★	USB/NFC physical key plugged in or tapped	Highest-value: email, bank, password manager
Authenticator app	★★★★	Generates rotating 6-digit codes	Almost everything else
Push notification (Duo)	★★★★	Tap 'Approve' on a phone notification	Work / corporate accounts
Email-based code	★★	Code emailed to recovery address	Low-priority accounts only
SMS / text code	★	Code sent via text message	When nothing else is offered
Security questions	★ (low)	Answers to personal questions	Never as a primary method

Why SMS Is Weaker Than You Think

SMS-based MFA can be defeated by SIM swapping: an attacker calls your phone carrier, impersonates you, and convinces the carrier to transfer your number to their SIM. They now receive your text codes. SIM swaps happen routinely against high-value targets. Authenticator apps and hardware keys aren't vulnerable to this. Migrate critical accounts off SMS where possible.

The 5 Authenticator Apps Worth Using

- **Authy** — multi-device, encrypted cloud backup, easy to use. Solid choice.
- **2FAS** — open-source, multi-device, encrypted backup. Privacy-friendly.
- **Google Authenticator** — added cloud sync in 2023, available on Android and iOS.
- **Microsoft Authenticator** — strong if you're in the Microsoft ecosystem.
- **Built-in to your password manager** — convenient but couples 2FA to PM access.

Setting Up MFA On Your Email — The 10-Minute Walkthrough

1. Install your chosen authenticator app on your phone.
2. Go to your email's Security settings (Gmail: myaccount.google.com → Security; Outlook: account.microsoft.com → Security).
3. Find 'Two-step verification' or '2-Step Verification.' Click 'Set up.'
4. Choose 'Authenticator app' as the method.
5. Scan the QR code with your authenticator app.
6. Enter the 6-digit code shown in the app to verify it works.
7. **Save the backup codes that appear next.** Store in your password manager Secure Notes AND on paper in a fire safe.
8. Sign out and sign back in to confirm MFA is active.

Migrating From SMS To Authenticator App

If you already use SMS-based MFA, the migration is straightforward: in the same Security settings, look for 'Add another method' or 'Switch primary method,' choose Authenticator app, complete setup. Then disable SMS as the primary method (some accounts force you to keep SMS as a backup — that's fine, just make sure authenticator is primary).

Recovery Codes — The Most Important Step

When you set up MFA, the service shows you a list of one-time recovery codes (usually 8-10 of them). These codes let you regain access if you lose your phone. **Save them immediately** — if you don't, and you lose your phone, you may be permanently locked out of your account.

Best practice for recovery code storage:

1. Save them in your password manager's Secure Notes (encrypted, accessible from any device).
2. Print them on paper and store in a fire safe.
3. Tell a trusted family member where the printed copy is (without showing them the codes).

Hardware Keys — Worth The Investment?

A hardware key (YubiKey 5 series, Google Titan) is a small USB or NFC device. You tap it to authenticate. They're immune to phishing, SIM swapping, and most other attacks. The downside: cost ($25-70 per key) and you need TWO (a primary and a backup) so you don't lock yourself out. For email, bank, password manager, and high-value work accounts, they're worth it. For everything else, an authenticator app is fine.

If You Lose Your Phone

- Use recovery codes to log into critical accounts from a different device.
- Disable old MFA setup, enable on new phone.
- If using Authy / 2FAS with cloud backup, sign in on the new phone and your codes appear.
- If using Google Authenticator without cloud sync, you'll need to re-enrol each account using recovery codes.
- Set up the new phone, enable MFA, store new recovery codes, repeat.

Where To Go Next

- **Use the Two-Factor Authentication Cheat Sheet** — quick hierarchy reference.
- **Use the Password Security Checklist** — pair MFA with strong unique passwords.
- **Read the Beginner's Guide to Password Managers** — they work together.