

Multi-Factor Authentication (MFA)

Understanding account protection and a step-by-step setup guide

1. What is Multi-Factor Authentication?

Multi-Factor Authentication (MFA) is a security mechanism that requires users to provide two or more distinct verification factors before gaining access to an online account, application, or system. Instead of relying solely on a password—which can be stolen, guessed, or leaked—MFA adds critical extra layers of defense.



1. Something You Know

Knowledge-based credentials such as passwords, PINs, or answers to security questions.



2. Something You Have

Physical or digital items, such as an authenticator app, hardware key (YubiKey), or SMS code.



3. Something You Are

Biometric attributes unique to you, such as fingerprint scans, facial recognition, or iris scans.



Why is MFA Crucial?

Over 80% of data breaches involve weak, reused, or compromised passwords. Enabling MFA blocks more than **99% of automated account takeover attacks**, ensuring that even if a hacker knows your password, they still cannot access your account.

2. Step-by-Step Setup Guide

Setting up MFA takes less than 5 minutes. Follow these standard steps applicable to almost any platform (e.g., Google, Microsoft, Apple, Banking apps):

1 Download an Authenticator App

Recommended Method

Install a trusted authenticator app on your smartphone from the official App Store (iOS) or Google Play Store (Android):

- **Popular Options:** Google Authenticator, Microsoft Authenticator, 1Password, or Authy.
- **Note:** Authenticator apps are significantly more secure than SMS text messages, which can be intercepted via SIM-swapping.

2 Navigate to Account Security Settings

Log into the service you want to secure (e.g., email, social media, bank) on your computer or tablet:

- Go to **Settings** or **Account Settings**.
- Look for **Security**, **Sign-in & Security**, or **Two-Factor Verification (2FA/MFA)**.

3 Enable MFA & Scan the QR Code

Click "**Turn on 2-Step Verification**" or "**Add Authentication App**":

- A **QR Code** will appear on your computer screen.
- Open your smartphone's Authenticator App, tap the "+" button, and choose "**Scan a QR Code**".
- Point your phone camera at the computer screen to link the account.

4 Confirm with a Verification Code

Once scanned, your mobile app will display a temporary 6-digit numeric code that changes every 30 seconds. Enter this code into the website prompt to confirm the successful link.

5 Save Backup / Recovery Codes

The service will generate a set of one-time **Backup/Recovery Codes**:

- **Action required:** Copy or print these codes and store them in a secure place (e.g., a password manager or physical safe).
- These codes allow you to regain access to your account if you ever lose or break your mobile phone.

Security Best Practice Tip

Prioritize setting up MFA on your primary email address first. Since password resets for all other online accounts are sent to your main email, securing it protects your entire digital footprint.