

Multi-Factor Authentication (MFA) Setup Instructions

What is Multi-Factor Authentication?

Multi-Factor Authentication (MFA) adds an extra layer of security to your accounts by requiring two or more verification methods: 1. Something you know (password) 2. Something you have (phone or security key) 3. Something you are (fingerprint or face)

Why Use MFA?

- Protects your account even if your password is compromised
- Prevents unauthorized access from hackers
- Alerts you to potential break-in attempts
- Required by many financial institutions and email providers

Setting Up MFA on Common Services

Gmail / Google Account

1. Sign in to your Google Account at accounts.google.com
2. In the navigation panel, click **Security**
3. Under "Signing in to Google," click **2-Step Verification**
4. Click **Get started**
5. Follow the on-screen steps to set up text message verification
6. Enter the verification code sent to your phone
7. Click **Turn on** to enable 2-Step Verification

Yahoo Mail

1. Sign in to your Yahoo account
2. Click on your name or profile icon in the upper right corner
3. Select **Account info**
4. Click **Account security** in the left sidebar
5. Click **Two-step verification** and toggle it **On**
6. Enter your phone number and click **Send code**
7. Enter the verification code sent to your phone
8. Click **Verify** to complete setup

Microsoft Account (Outlook, Hotmail)

1. Sign in to your Microsoft account at account.microsoft.com
2. Select **Security** from the top navigation bar
3. Select **Advanced security options**
4. Under "Two-step verification," select **Turn on**
5. Follow the on-screen instructions to set up your verification method
6. Enter the code sent to your phone
7. Click **Next** and then **Finish** to complete setup

Facebook

1. Sign in to your Facebook account
2. Click the down arrow in the top right corner
3. Select **Settings & Privacy**, then **Settings**
4. Click **Security and Login** in the left sidebar
5. Scroll to "Two-Factor Authentication" and click **Edit**
6. Select **Text Message (SMS)** as your security method
7. Enter your phone number and click **Continue**
8. Enter the code sent to your phone
9. Click **Continue** to complete setup

Setting Up Backup Methods

Recovery Codes

1. During MFA setup, most services offer recovery codes
2. Write these codes down on paper and store in a secure location
3. Keep a copy with your important documents
4. Never store recovery codes digitally without encryption

Backup Phone Number

1. Add a trusted family member's phone number as a backup
2. During MFA setup, look for "Add backup method" or similar option
3. Select "Add phone number" and enter the backup number
4. Verify the number by entering the code sent to that phone

Backup Email

1. Add a secondary email address to your account

2. Look for "Recovery email" or "Alternate email" in account settings
3. Enter a different email address that you can access
4. Verify by clicking the link sent to that email address

Troubleshooting MFA Issues

Lost Phone

1. Use your recovery codes to sign in
2. If you don't have recovery codes, use your backup phone number
3. As a last resort, contact the service's customer support

New Phone

1. Sign in using your old phone before switching
2. Update your MFA settings with your new phone number
3. If you've already switched phones, use recovery codes to sign in

No Cell Phone

If you don't have a cell phone, alternative options include: 1. Email verification (where available) 2. Authentication apps on tablets or iPods 3. Printed backup codes 4. Security keys (physical USB devices)

Remember

- Always set up backup methods when enabling MFA
- Print and securely store recovery codes
- Update your MFA settings when you change phone numbers
- Test your recovery methods before you need them