
RESOURCE 02 | DON'T CLICK YET COMPANION RESOURCE

MFA Setup Tracker

Companion resource for Don't Click Yet. Referenced on page 79.

Purpose: Track which important accounts have multi-factor authentication enabled and where you still need to act.

Storage reminder: If you complete this worksheet with sensitive information, store the finished copy somewhere safe.

Multi-factor authentication, often shortened to MFA, adds a second layer of protection to an account. A password proves one thing: that someone knows the password. MFA asks for another proof, such as a code, device approval, passkey, authenticator app, or security key.

MFA is especially important for accounts that protect money, identity, communication, recovery, or important files. Start with your main email account, bank, password manager, phone provider, cloud storage, Apple/Google/Microsoft account, payment apps, and health or business accounts.

Use this tracker to record which accounts have MFA, what method is used, where backup codes are stored, and what you would do if your phone or authentication device were lost.

Do not write actual MFA codes on this worksheet. Codes change and should not be saved here. If an account provides backup codes, store them securely and use this worksheet only to record where they are stored.

MFA Priority List

Begin with the accounts that would cause the most trouble if someone else accessed them.

Check the accounts you need to review:

- Main email account
- Password manager
- Bank account
- Credit card account
- Mobile phone provider
- Apple account
- Google account
- Microsoft account
- Cloud storage
- Payment apps
- Health portal
- Insurance account
- Tax or government account
- Social media account
- Business email
- Business banking
- Website hosting or domain account
- Accounting or invoicing platform
- Other: _____

MFA Methods

Different accounts may offer different MFA methods. Some are stronger than others, but the best method is one you can use consistently and recover safely.

Common MFA methods include:

- **Authenticator app:** An app that generates temporary codes.
- **Device prompt:** A sign-in approval prompt on a trusted device.
- **Passkey:** A newer sign-in method tied to a device or account.
- **Security key:** A physical device used to approve sign-ins.
- **Text message code:** A code sent by SMS.
- **Email code:** A code sent to an email address.
- **Backup codes:** One-time recovery codes provided by the account.
- **Recovery contact:** A trusted person or account used for recovery.

Text-message codes are better than having no MFA, but they may be less secure than authenticator apps, passkeys, or security keys. Use the strongest method you can manage reliably.

Main Email Account

Account or provider:

Email address or username:

MFA turned on?

☐ Yes

☐ No

☐ Not sure

MFA method used:

☐ Authenticator app

☐ Device prompt

☐ Passkey

☐ Security key

☐ Text message code

☐ Email code

☐ Other: _____

Backup codes provided?

☐ Yes

☐ No

☐ Not sure

Backup codes stored where:

Recovery phone number:

Recovery email address:

Trusted devices reviewed?

- ☐ Yes
☐ No
☐ Not sure

Date reviewed:

Notes:

Password Manager

Password manager name:

Account email or username:

MFA turned on?

- ☐ Yes
☐ No
☐ Not sure

MFA method used:

- ☐ Authenticator app
☐ Security key
☐ Passkey
☐ Device prompt
☐ Text message code
☐ Other: _____

Backup codes provided?

- ☐ Yes
☐ No
☐ Not sure

Backup codes stored where:

Emergency access or recovery method set up?

- ☐ Yes

- ☐ No
☐ Not sure

Trusted emergency contact, if any:

Date reviewed:

Notes:

Bank Account

Bank name:

Account username or email:

MFA turned on?

- ☐ Yes
☐ No
☐ Not sure

MFA method used:

- ☐ Authenticator app
☐ Device prompt
☐ Passkey
☐ Security key
☐ Text message code
☐ Email code
☐ Phone call
☐ Other: _____

Backup codes provided?

- ☐ Yes
☐ No
☐ Not sure

Backup codes stored where:

Transaction alerts enabled?☐ Yes☐ No☐ Not sure**Trusted support route:**

Date reviewed:

Notes:

Credit Card Account**Card issuer:**

Account username or email:

MFA turned on?☐ Yes☐ No☐ Not sure**MFA method used:**☐ Authenticator app☐ Device prompt☐ Passkey☐ Security key☐ Text message code☐ Email code☐ Phone call☐ Other: _____**Backup codes provided?**☐ Yes☐ No☐ Not sure**Backup codes stored where:**

Transaction alerts enabled?☐ Yes☐ No☐ Not sure**Trusted support route:**

Date reviewed:

Notes:

Mobile Phone Provider

Your phone provider account matters because your phone number may receive verification codes and recovery messages.

Provider name:

Account phone number:

MFA turned on?☐ Yes☐ No☐ Not sure☐ Not available**MFA method used:**☐ Authenticator app☐ Device prompt☐ Passkey☐ Security key☐ Text message code☐ Email code☐ Account PIN☐ Other: _____

Account PIN set?☐ Yes☐ No☐ Not sure**Port-out protection, number lock, or transfer protection enabled?**☐ Yes☐ No☐ Not sure☐ Not available**Backup codes or recovery information stored where:**

Trusted support route:

Date reviewed:

Notes:

Apple, Google, or Microsoft Account

These accounts may control email, device backup, app stores, cloud storage, photos, documents, subscriptions, and lost-device tools.

Provider:☐ Apple☐ Google☐ Microsoft☐ Other: _____**Account email:**

MFA turned on?☐ Yes☐ No☐ Not sure**MFA method used:**☐ Authenticator app☐ Device prompt☐ Passkey

-
- ☐ Security key
 - ☐ Text message code
 - ☐ Email code
 - ☐ Recovery contact
 - ☐ Other: _____

Backup codes provided?

- ☐ Yes
- ☐ No
- ☐ Not sure

Backup codes stored where:

Recovery phone number:

Recovery email address:

Trusted devices reviewed?

- ☐ Yes
- ☐ No
- ☐ Not sure

Lost-device feature enabled?

- ☐ Yes
- ☐ No
- ☐ Not sure

Date reviewed:

Notes:

Cloud Storage or Backup Account**Service name:**

Examples: iCloud, Google Drive, OneDrive, Dropbox, Backblaze, Carbonite, or another backup provider.

Account email:

MFA turned on?

☐ **Yes**

☐ **No**

☐ **Not sure**

MFA method used:

☐ Authenticator app

☐ Device prompt

☐ Passkey

☐ Security key

☐ Text message code

☐ Email code

☐ Other: _____

Backup codes provided?

☐ **Yes**

☐ **No**

☐ **Not sure**

Backup codes stored where:

Recovery phone number or email:

Last successful backup or sync check:

Last recovery test:

Date reviewed:

Notes:

Payment App

Use this section for PayPal, Venmo, Cash App, Zelle access through a bank, Apple Cash, Google Pay, or another payment service.

Payment app name:

Account email or phone number:

MFA turned on?

- ☐ Yes
- ☐ No
- ☐ Not sure
- ☐ Not available

MFA method used:

- ☐ Authenticator app
- ☐ Device prompt
- ☐ Passkey
- ☐ Security key
- ☐ Text message code
- ☐ Email code
- ☐ App PIN or biometric lock
- ☐ Other: _____

Backup codes provided?

- ☐ Yes
- ☐ No
- ☐ Not sure

Backup codes stored where:

Linked bank or card reviewed?

- ☐ Yes
- ☐ No
- ☐ Not sure

Alerts enabled?

- ☐ Yes
- ☐ No
- ☐ Not sure

Date reviewed:

Notes:

Health Portal

Health system or provider:

Portal name:

Account email or username:

MFA turned on?

☐ Yes

☐ No

☐ Not sure

☐ Not available

MFA method used:

☐ Authenticator app

☐ Device prompt

☐ Passkey

☐ Security key

☐ Text message code

☐ Email code

☐ Phone call

☐ Other: _____

Recovery email or phone:

Trusted person authorized to help, if applicable:

Date reviewed:

Notes:

Social Media Account

Social media accounts can be used to impersonate you, contact family, spread scams, or damage your reputation.

Platform:

Username or account email:

MFA turned on?

☐ Yes

☐ No

☐ Not sure

MFA method used:

☐ Authenticator app

☐ Device prompt

☐ Passkey

☐ Security key

☐ Text message code

☐ Email code

☐ Other: _____

Backup codes provided?

☐ Yes

☐ No

☐ Not sure

Backup codes stored where:

Recovery email or phone:

Trusted contact if account is compromised:

Date reviewed:

Notes:

Business or Freelance Account

Use this section for accounts connected to business email, client files, website hosting, domain registration, accounting software, invoicing, professional platforms, or cloud storage.

Account or platform:

Business purpose:

Account email or username:

MFA turned on?

☐ Yes

☐ No

☐ Not sure

MFA method used:

☐ Authenticator app

☐ Device prompt

☐ Passkey

☐ Security key

☐ Text message code

☐ Email code

☐ Other: _____

Backup codes provided?

☐ Yes

☐ No

☐ Not sure

Backup codes stored where:

Client, financial, or sensitive data stored here?

☐ Yes

☐ No

☐ Not sure

Trusted person or professional who can help:

Date reviewed:

Notes:

Additional MFA Account Tracker

Use this section for any other account where MFA matters.

Account	Username or Email	MFA Method	Backup Codes Stored Where	Date Reviewed	Notes

Lost Phone or MFA Device Plan

Many MFA methods depend on your phone or another device. Prepare before that device is lost, stolen, broken, replaced, or erased.

If I lose my phone, I will first:

Device or account I will use to locate or lock the phone:

Where backup codes are stored:

Trusted person who can help:

Accounts that depend most heavily on this phone:

1.

2.

3.

4. _____
5. _____

Before replacing or wiping my phone, I will check:

- Authenticator app transfer or backup.
- Passkeys stored on the device.
- Trusted-device prompts.
- Password manager access.
- Apple, Google, or Microsoft account access.
- Banking app access.
- Payment app access.
- Cloud photo and contact backup.
- Recovery codes for critical accounts.

Backup Code Storage

Backup codes are important because they may help you regain access if your MFA device is unavailable. Store them somewhere safe and retrievable.

Possible storage options include:

- Password manager secure note
- Printed copy in a safe
- Encrypted digital file
- Sealed emergency envelope
- Attorney or estate-planning file
- Secure family emergency folder

Avoid leaving backup codes in plain view, in an unprotected note app, in email drafts, or in a photo on your phone.

My backup code storage method:

Trusted person who knows where emergency backup codes are stored, if applicable:

Review Log

Review MFA settings at least once a year and whenever you replace your phone, change phone numbers, change email addresses, change banks, set up a new password manager, or add a major account.

Review date: _____

Reviewed by: _____

Changes made: _____

Review date: _____
Reviewed by: _____
Changes made: _____

Review date: _____
Reviewed by: _____
Changes made: _____

Final Reminder

MFA is most useful when you understand the situation in which it appears.

Use codes only when you are signing in or making a change through a process you started. Do not read, text, forward, or approve codes for someone who contacts you unexpectedly.

A real code can still be part of a fake request.