How to: Increase user account security with multi-factor authentication

Formerly known as **Two-Factor Authentication**, or 2FA, **Multi-Factor Authentication**, or MFA, protects your user account from unauthorized access by requiring you to verify your identity with an additional credentials. When you sign into your account, you will use your **ActionID** email and password, and then you'll be required to enter a **Verification Code** sent to your phone or found in a mobile authenticator app, depending on which type of MFA you've set up.

After setting up MFA, **be sure to download your recovery code**. Having this code easily accessible will be essential for logging in when you do not have access to your mobile device or MFA is not working for any reason.

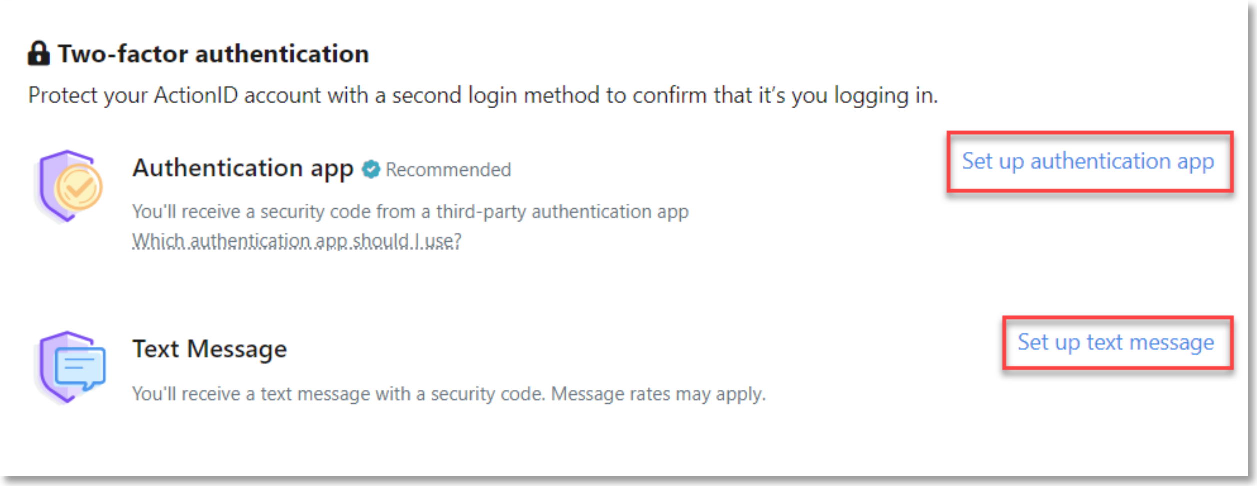
Using MFA makes your data more secure by preventing bad actors from gaining access to your CRM so it's best practice for all users to enable MFA. The more access someone has to sensitive data or tasks, the more important it becomes. At a minimum, setting up MFA is a good idea for users who:

- have access to sensitive data, such as donor profiles or Scores
- are able to perform more sensitive tasks, like sending emails or Bulk Uploading (importing data)
- have the ability to export
- have access to API integrations

Setting up MFA

To enable MFA for your ActionID, go to https://myaccount.ngpvan.com and follow these steps:

1. Log in with your **ActionID**
2. Navigate to your ActionID Account
3. Navigate to the Two-factor Authentication option box
4. Select one of the two options:
   - **Set up with Authenticator App** (recommended)
   - **Set up with phone number**



Two-factor authentication

Protect your ActionID account with a second login method to confirm that it's you logging in.

Authentication app Recommended

You'll receive a security code from a third-party authentication app

Which authentication app should I use?

Set up authentication app

Text Message

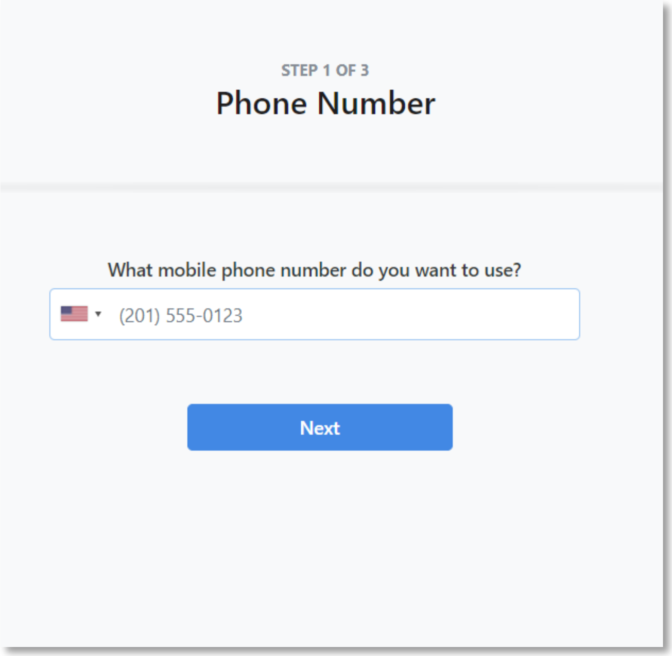
You'll receive a text message with a security code. Message rates may apply.

Set up text message

Setting up MFA With Phone Number

If you choose to set up MFA with a phone number, follow these steps to have a code sent to your phone:

1. Verify the phone number associated with your **ActionID** is correct.
2. Click **Send Code.**



STEP 1 OF 3

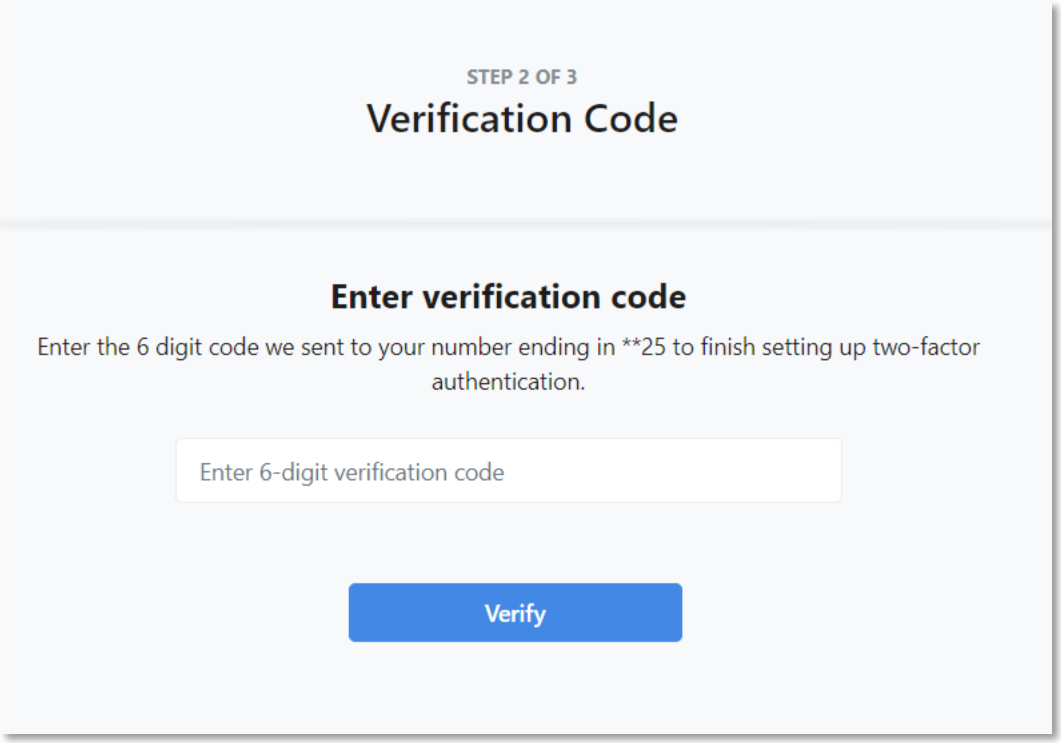
Phone Number

What mobile phone number do you want to use?

(201) 555-0123

Next

3. Enter the **Verification Code** sent to your phone and click **Verify.**



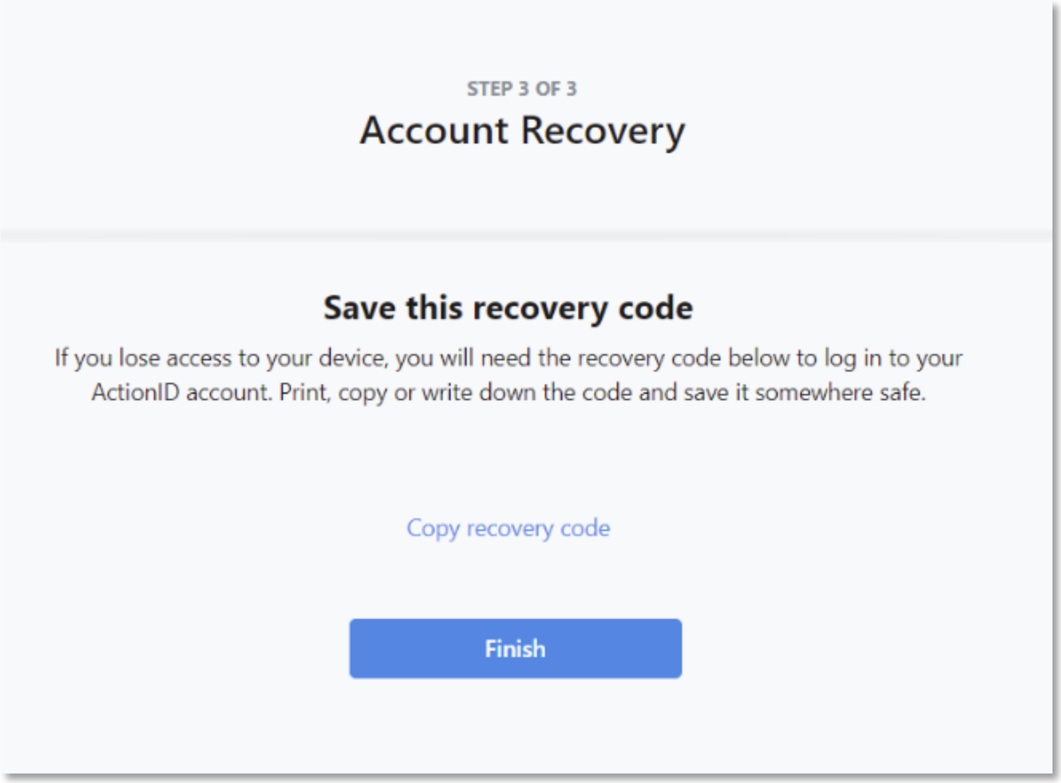
STEP 2 OF 3

Verification Code

Enter verification code

Enter the 6 digit code we sent to your number ending in **25 to finish setting up two-factor authentication.

4. Save your Account Recovery Code in case you lose access to your device.



STEP 3 OF 3

Account Recovery

Save this recovery code

If you lose access to your device, you will need the recovery code below to log in to your ActionID account. Print, copy or write down the code and save it somewhere safe.

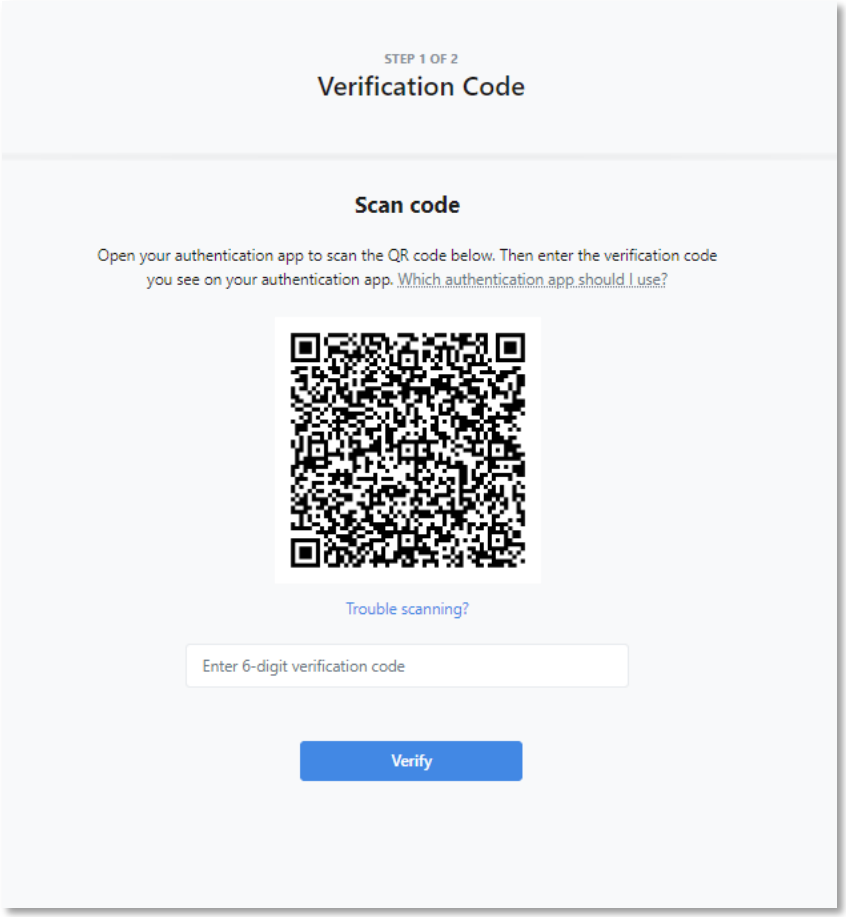
Multi-factor authentication should now be enabled for your **ActionID**. The next time you log in with your **ActionID** and password, a similar code will be texted to you, and you will enter that code on your screen to finish logging in.

Setting up MFA with Authenticator App

If you select the option to enable MFA with an authenticator app, you will need to download an authenticator app of your choice. Most common authenticator apps will work with **ActionID**, including LastPass and Authy.

Once you have downloaded an authenticator app, follow these steps:

1. Scan the QR code on your computer screen.



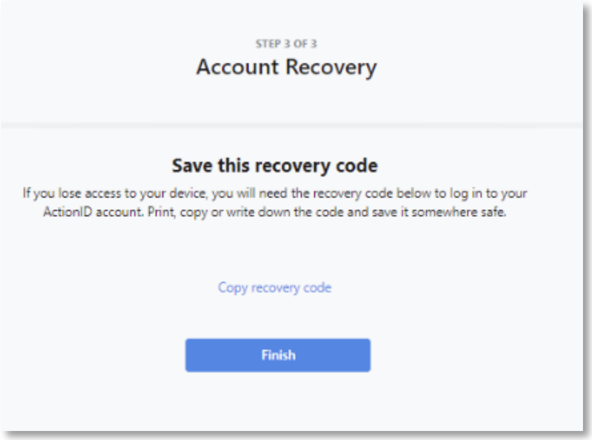
STEP 1 OF 2

Verification Code

Scan code

Open your authentication app to scan the QR code below. Then enter the verification code you see on your authentication app. Which authentication app should I use?

2. Check the app on your phone for a code.
3. Enter the code in the **Verification Code** field.
4. Click **Enable.**
5. Save your Account Recovery Code in case you lose access to your device.



STEP 3 OF 3

Account Recovery

Save this recovery code

If you lose access to your device, you will need the recovery code below to log in to your ActionID account. Print, copy or write down the code and save it somewhere safe.

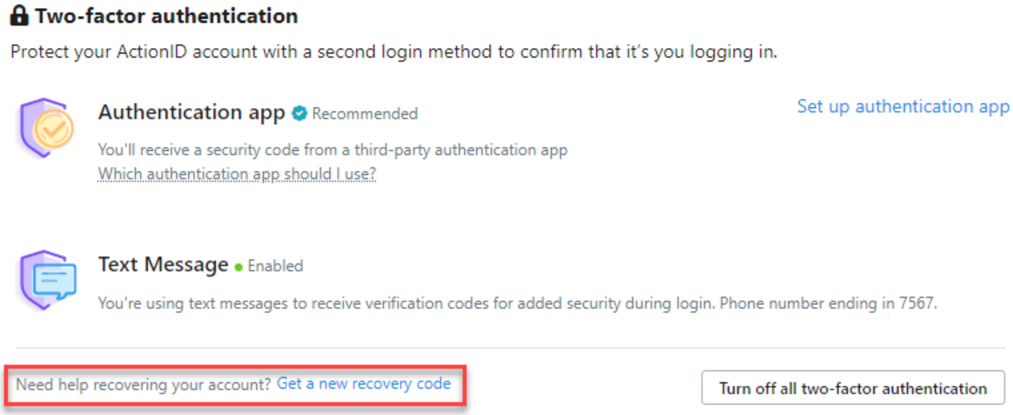
The next time you log in with your **ActionID** and password, you will need to open your app to view the code, and enter it on your screen to finish logging in. This will happen every 30 days or if you use a new browser or device.

Downloading your recovery code

Recovery codes provide you with an alternative way to log in if you do not have access to your phone, are not receiving the text with the **Verification Code**, or the authenticator app is not working. While it may be tempting to put off downloading your recovery code, it's best to avoid a stressful situation later on by downloading them immediately.

To get your recovery code, follow these steps:

1. Go to https://myaccount.ngpvan.com/.
2. Click **Edit Profile.**
3. Enter ActionID credentials.
4. Click **Log in.**
5. Click **Get a new recovery code.**



Two-factor authentication

Protect your ActionID account with a second login method to confirm that it's you logging in.

Authentication app ✓ Recommended

You'll receive a security code from a third-party authentication app

Which authentication app should I use?

Text Message ● Enabled

You're using text messages to receive verification codes for added security during login. Phone number ending in 7567.

Need help recovering your account? Get a new recovery code

Set up authentication app
Turn off all two-factor authentication

6. Print, copy, or write down the code.
7. Click **Finish.**

Store this code somewhere you will remember, keeping in mind that you may need them a year or two down the road. If you use a password manager like LastPass or 1Password, consider storing them there.

If you do not have your recovery code, you will need to reach out to your administrator, who will send a request to our Support Team to reset your **ActionID**. This can be inconvenient and prevent you from getting things done, but is easily avoidable by downloading and storing your recovery code.

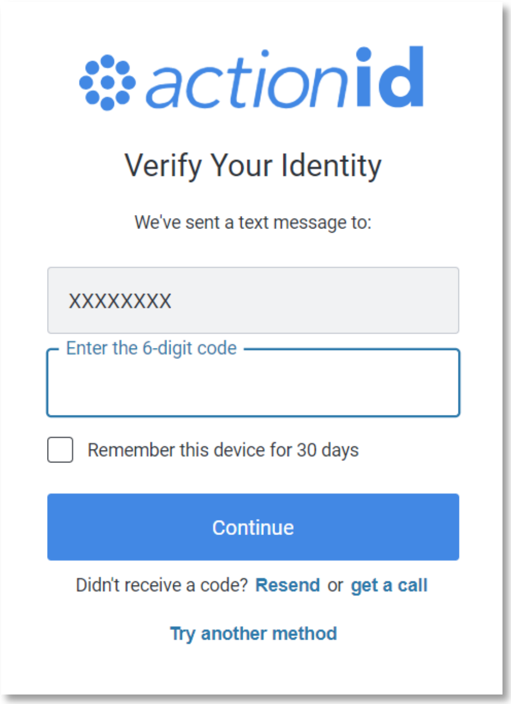
Logging in with MFA

Once you've enabled MFA, you will be prompted to enter a code after entering your ActionID email and password, each time you log in.

You will also be given the option to **Remember this device**. If you check this box, you will not have to complete two-step verification *from that device and browser combination* for 30 days. You will be prompted for MFA again if:

- you log in from that browser and device after the 30 days have passed
- you clear your browser cookies at any time
- you log in from another browser or device at any time

Remembering the device is only suggested for personal devices that are not shared. You should never check this box for shared or public devices, such as library computers or devices lent to you by a campaign or organization.



Verify Your Identity

We've sent a text message to:

XXXXXXXX

Enter the 6-digit code

☐ Remember this device for 30 days

Didn't receive a code? Resend or get a call

If you no longer have access to that mobile device, you can select **Use a recovery code** > enter a recovery code > **Verify**. Keep in mind that the screen that you see after clicking on the recovery code link will look almost identical to the previous screen. The only different is that it will say **Enter a recovery code that you have saved** instead of prompting you to enter the regular MFA verification code.

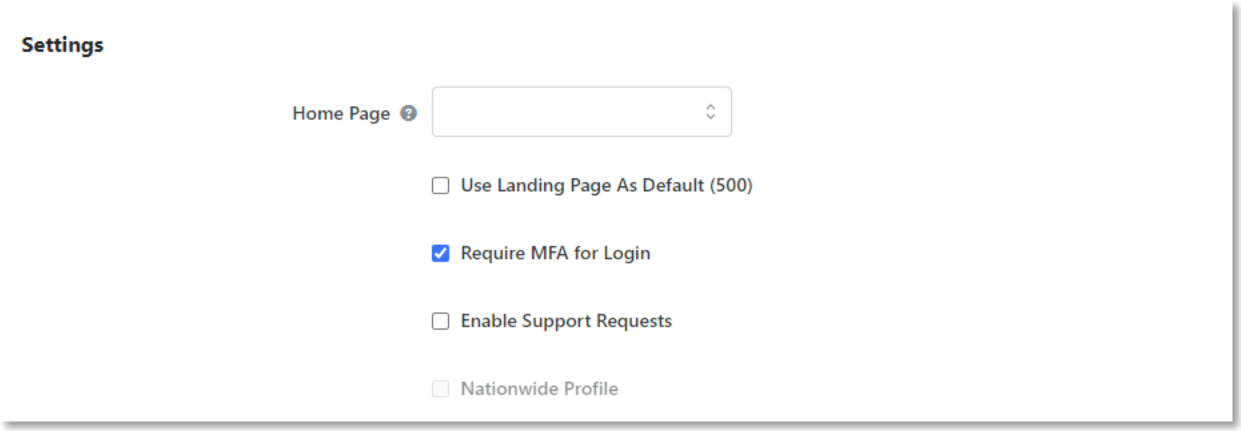
Requiring MFA for other users

If you are creating user accounts for others, you may want to make their user account more secure by requiring that they use MFA to log in. This becomes more important when:

- A user has access to sensitive data, such as donor profiles or Scores
- A user is able to perform more sensitive tasks, like sending emails or Bulk Uploading (importing data)
- A user has the ability to export
- A user has access to API integrations

You can require MFA for other users at the **User Profile** level, meaning that you will edit the **User Profile** settings and then all users with that **User Profile** will be required to set up and use MFA the next time they log in.

To require MFA for users with particular **User Profiles**, check the **Require MFA for Login** checkbox in the **Settings** section. You can do this when creating a **User Profile** or editing an existing one. If you're updating an existing one, users with that profile will be prompted to set up MFA the next time they log in.



Settings

Home Page

□ Use Landing Page As Default (500)

☑ Require MFA for Login

□ Enable Support Requests

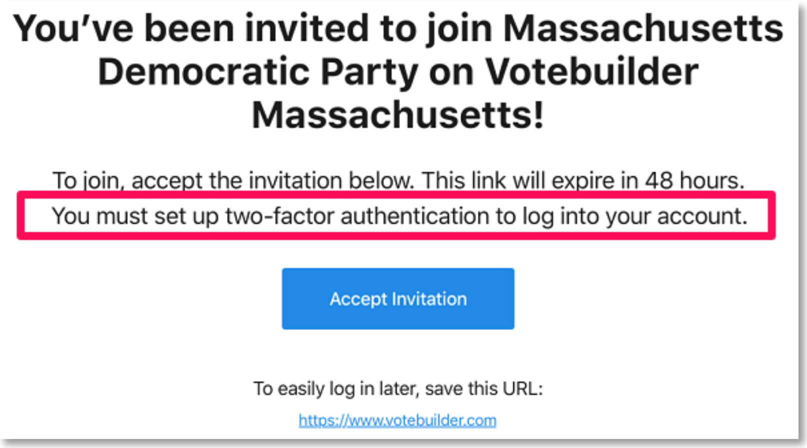
□ Nationwide Profile

It's a good idea to let users know that they will be prompted to set up MFA, and to remind them how important it is to download their recovery code.

Please keep in mind that users logging in at some sites may not have the ability to create and edit **User Profiles**, and instead have pre-set ones; in such cases, support staff will enable it for **User Profiles** when necessary.

What your users will see

If a user account has a User Profile that requires MFA, they will see a note in their **ActionID** invitation (i.e. their login invitation).

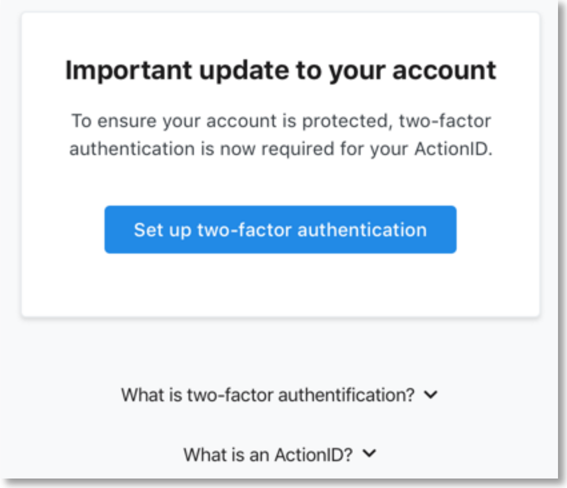


You've been invited to join Massachusetts Democratic Party on Votebuilder Massachusetts!

To join, accept the invitation below. This link will expire in 48 hours.
You must set up two-factor authentication to log into your account.

To easily log in later, save this URL:
https://www.votebuilder.com

If a user attempts to log in without setting up MFA, they will see a prompt to do so before they can access the database. The link will take them to their **ActionID** profile page, where they can enable it.



Important update to your account

To ensure your account is protected, two-factor authentication is now required for your ActionID.

Set up two-factor authentication
What is two-factor authentification?
What is an ActionID?