

# renci SelfService

## PASSWORD/PASSPHRASE MANAGEMENT GUIDE

## Table of Contents

Enrollment.....	2
Steps to Enroll: .....	2
Password Management .....	4
Minimum Password Complexity Requirements.....	4
Change Your RENCI Account Password/Passphrase .....	4
Reset Your RENCI Account Password/Passphrase .....	5
Multi-Factor Authentication (MFA) Methods.....	6
Email Verification Code .....	6
Security Questions & Answers .....	6
Duo.....	6
MFA Recovery .....	8

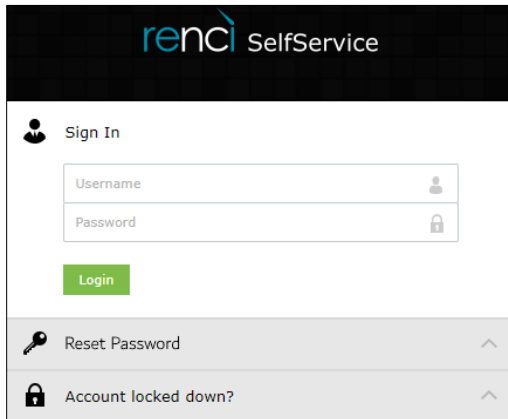
## Enrollment

Enrollment is mandatory and will allow you to reset/change your password or passphrase, using RENCI SelfService.

A one-time process, enter a verification code that is sent to your RENCI email address (for external users, the email you used when signing up for an account) after logging in to the RENCI SelfService portal for the first time.

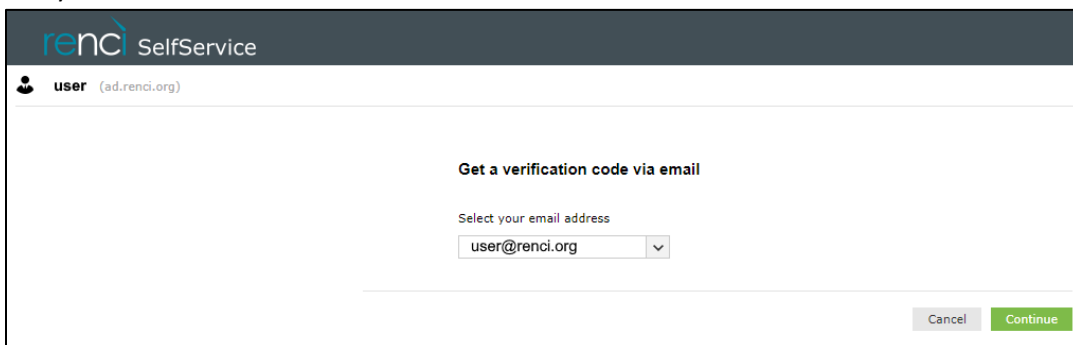
### Steps to Enroll:

1. In your browser, go to RENCI SelfService (<https://selfservice.renci.org>)
2. Login, using your RENCI credentials.



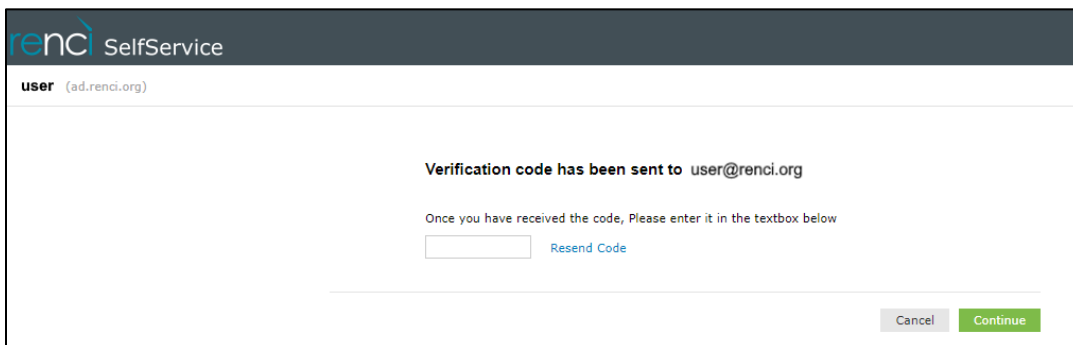
The screenshot shows the 'renci SelfService' login interface. It features a 'Sign In' section with input fields for 'Username' and 'Password', and a green 'Login' button. Below the login fields are two links: 'Reset Password' and 'Account locked down?', each with an upward-pointing arrow.

3. The next page prompts you to "Get a verification code via email". Your email address will be populated automatically. Click **Continue**.



The screenshot shows the 'Get a verification code via email' page. The user is identified as 'user (ad.renci.org)'. The page prompts the user to 'Select your email address' with a dropdown menu showing 'user@renci.org'. At the bottom right, there are 'Cancel' and 'Continue' buttons.

4. Enter the **verification code** that was sent to the above email address. Click **Continue**.



The screenshot shows the verification code entry page. The user is identified as 'user (ad.renci.org)'. The page displays the message 'Verification code has been sent to user@renci.org' and prompts the user to 'Once you have received the code, Please enter it in the textbox below'. There is an input field for the code and a 'Resend Code' link. At the bottom right, there are 'Cancel' and 'Continue' buttons.


5. Upon successful email identity verification, you will be routed to the **Enrollment** tab of RENCi SelfService. Here, you will be able to manage your enrolled verification methods. Your Email Verification is one of the methods.

On this tab, you will also be able to setup alternative verification methods/Multi-Factor Authentication (MFA). **It is strongly recommended that you take the time to set up at least one additional MFA method.**


### Set Up Backup Verification Methods

These methods will help you prove your identity in case you face issues with other verification methods.

---

 **Security Questions & Answer**  
Answer the security questions to enroll. Prove your identity by answering the questions during SelfService and Logon actions.  
[Set up](#)

---

 **Duo Security**  
Prove your identity using the authentication method setup by your admin in Duo Security during SelfService and Logon actions.  
[Set up](#)

*\*\*If you experience any issues, during the enrollment process, please reach out to ACIS by submitting a Help Request to [help@renci.org](mailto:help@renci.org).\*\**

## Password Management

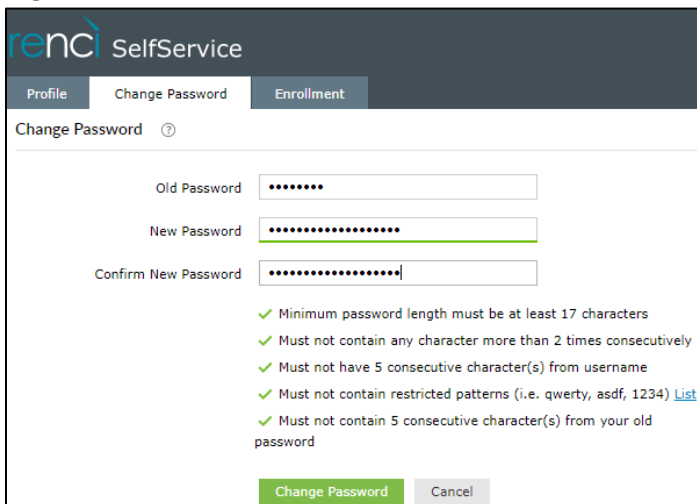
RENCI's Password Policy requires users to change their password **once a year (365 days)**. This is calculated from the time you last changed your password.

### Minimum Password Complexity Requirements

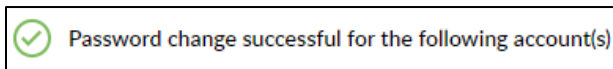
- Passwords/Passphrases changed every 365 days.
- Minimum password length should be at least 17.
- Must not contain any character more than 2 times consecutively.
- Must not have 5 consecutive characters from username.
- Must not contain 5 consecutive characters from your old password.
- Must not contain restricted patterns (i.e., qwerty, asdf, 1234)

### Change Your RENC Account Password/Passphrase

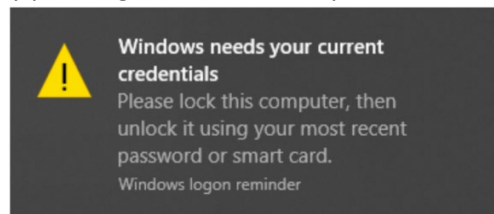
1. Login to RENC SelfService (<https://selfservice.renci.org>), using your preferred MFA method, and go to the **Change Password** tab.
2. Enter your existing password in the **Old Password** field.
3. Provide a **New Password** and re-enter it in the **Confirm New Password** field. Make sure your new password meets the complexity requirements.
4. Click **Change Password**.



5. If change is successful, you will receive the below message, as well as a confirmation email.



6. If you are a RENC employee with a company issued device, please make sure to complete the following:
  - **Windows Users:** To update the password on your Windows Device, sign onto RENC VPN using your new password. A notification should appear, saying "Windows needs your current credentials". Lock your device by pressing the Windows key + L, then enter your new credentials to unlock your device.



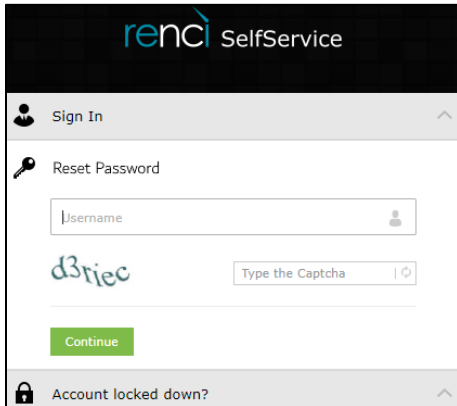
- **Mac Users:** Manually update your password on Mac OS X Key Chain if you have any shared drives configured.

**\*\*If you experience any issues, during the enrollment process, please reach out to ACIS by submitting a Help Request to [help@renci.org](mailto:help@renci.org).\*\***

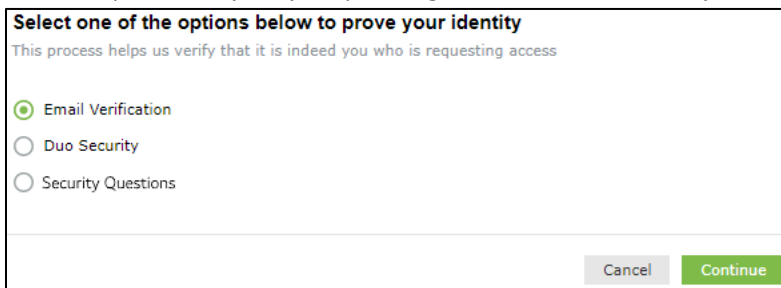
## Reset Your RENCI Account Password/Passphrase

If you have forgotten the password for your RENCI account -OR- if you are a new employee and need to set a new password, perform these steps:

1. In your browser, go to RENCI SelfService (<https://selfservice.renci.org>). Click **Reset Password?**
2. Enter your **username**.
3. Enter the **CAPTCHA verification code**.
4. Click **Continue**

A screenshot of the RENCI SelfService web interface. At the top, the logo 'renci SelfService' is displayed. Below it is a 'Sign In' header. The main section is titled 'Reset Password' and contains a 'Username' input field, a CAPTCHA image with the text 'd3tjcc', and a 'Type the Captcha' input field. A green 'Continue' button is positioned below the CAPTCHA. At the bottom of the page, there is a lock icon and the text 'Account locked down?'.

5. On the next page, you will be asked to choose an MFA method to prove your identity. Select one, then click **Continue**. *Your options may vary, depending on the MFA methods you have already configured.*

A screenshot of a page titled 'Select one of the options below to prove your identity'. Below the title is a subtitle: 'This process helps us verify that it is indeed you who is requesting access'. There are three radio button options: 'Email Verification' (which is selected), 'Duo Security', and 'Security Questions'. At the bottom right of the page are 'Cancel' and 'Continue' buttons.

6. After your MFA verification, on the next page, enter your **new password** and **confirm new password**, then click **Reset Password** to finish.

**\*\*If you experience any issues, during the enrollment process, please reach out to ACIS by submitting a Help Request to [help@renci.org](mailto:help@renci.org).\*\***

# Multi-Factor Authentication (MFA) Methods

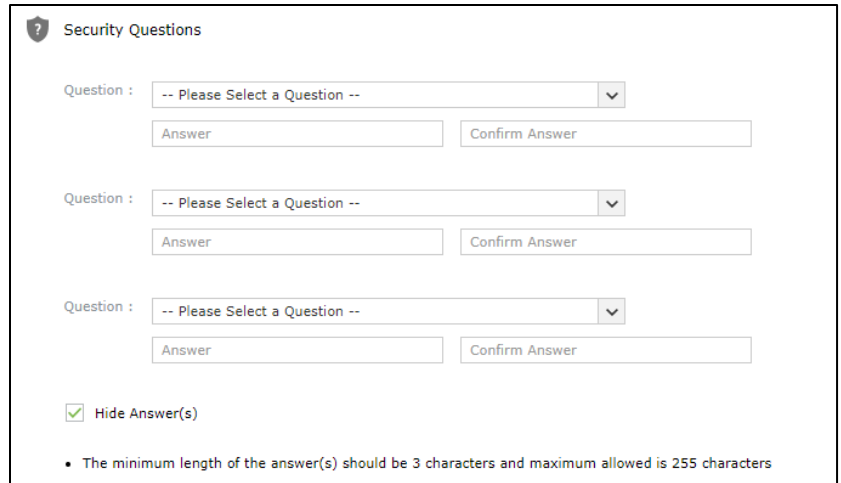
## Email Verification Code

This is the default method of MFA used when enrolling for the first time. A verification code is sent to the email address on file. Use this code to prove your identity when logging into the portal.

## Security Questions & Answers

You must provide valid answers to security questions to verify your identity. A set of three pre-defined security questions will be displayed. Choose the questions from the dropdown that you would like to use for authentication and then provide the appropriate answers.

In the RENCi SelfService portal, go to the **Enrollment** tab → **Security Questions & Answers** → **Set up**.



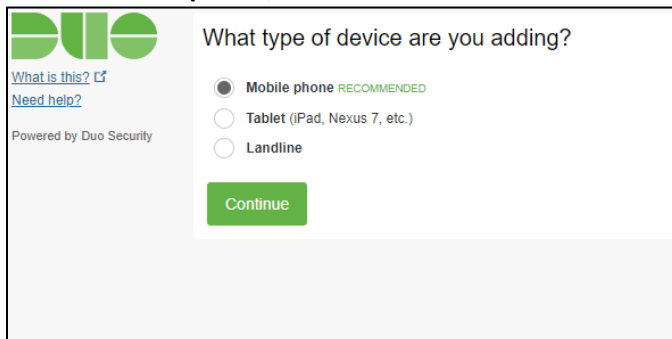
The screenshot shows a 'Security Questions' form with three identical rows. Each row contains a dropdown menu labeled 'Question : -- Please Select a Question --', an 'Answer' text input field, and a 'Confirm Answer' text input field. At the bottom of the form, there is a checked checkbox labeled 'Hide Answer(s)' and a note: 'The minimum length of the answer(s) should be 3 characters and maximum allowed is 255 characters'.

## Duo

Use the Duo Mobile Security push notification or code to verify your identity.

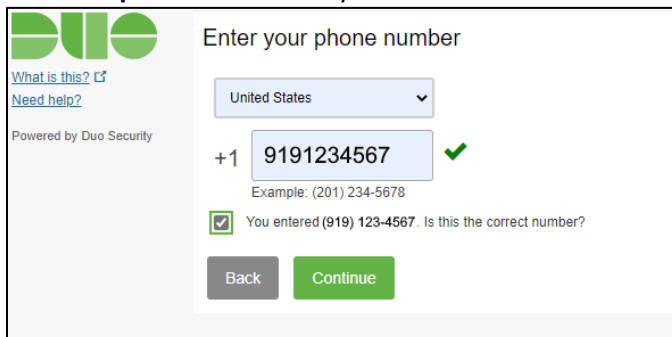
In the RENCi SelfService portal, go to the **Enrollment** tab → **Duo Security** → **Set up**.

1. Choose **Mobile phone, Continue**.



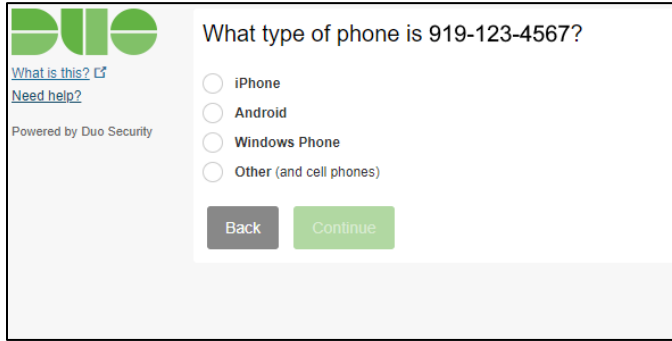
The screenshot shows the Duo Mobile selection screen. It features the Duo logo, a 'What is this?' link, a 'Need help?' link, and the text 'Powered by Duo Security'. The main heading is 'What type of device are you adding?'. There are three radio button options: 'Mobile phone RECOMMENDED' (selected), 'Tablet (iPad, Nexus 7, etc.)', and 'Landline'. A green 'Continue' button is at the bottom.

2. Enter the **phone number** of your mobile device. **Check** the box to verify your number. Click **Continue**.

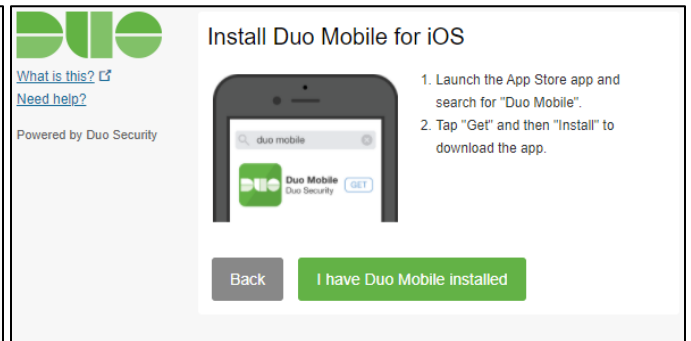
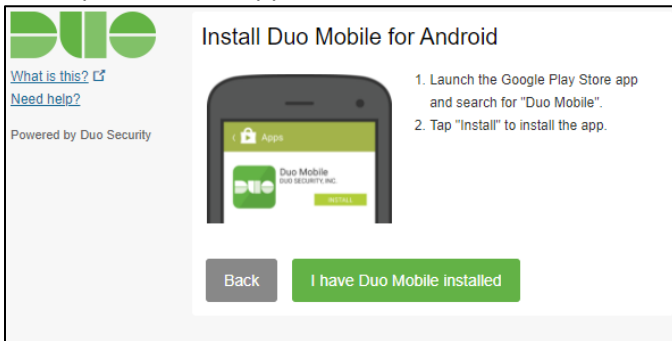


The screenshot shows the Duo Mobile phone number entry screen. It features the Duo logo, a 'What is this?' link, a 'Need help?' link, and the text 'Powered by Duo Security'. The main heading is 'Enter your phone number'. There is a dropdown menu for 'United States', a text input field for the phone number containing '+1 9191234567' with a green checkmark, and an example '(201) 234-5678'. Below the input field is a checked checkbox with the text 'You entered (919) 123-4567. Is this the correct number?'. At the bottom are 'Back' and 'Continue' buttons.

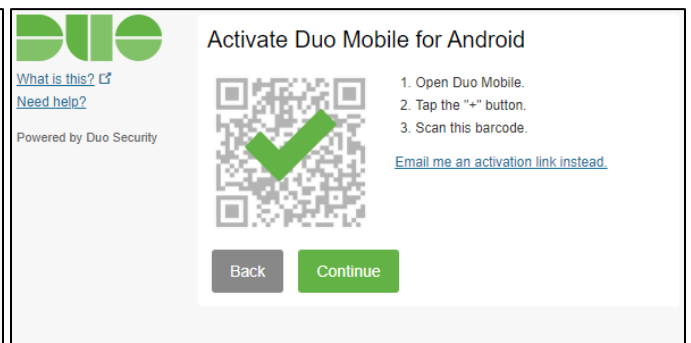
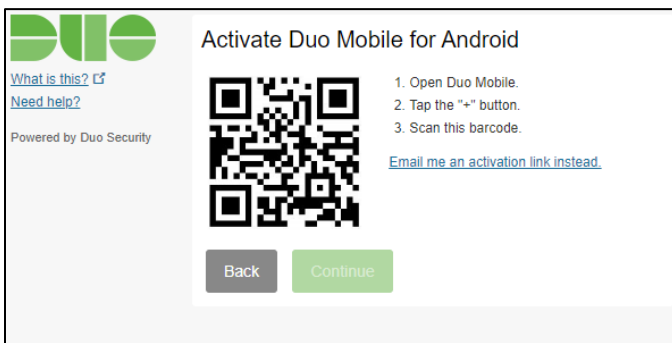
3. Choose your device **type**. Click **Continue**



4. Download the Duo Mobile app (if you don't have it already) from the [Google Play Store](#) or [Apple's App Store](#). When you have the app installed, click **I have Duo Mobile installed**.

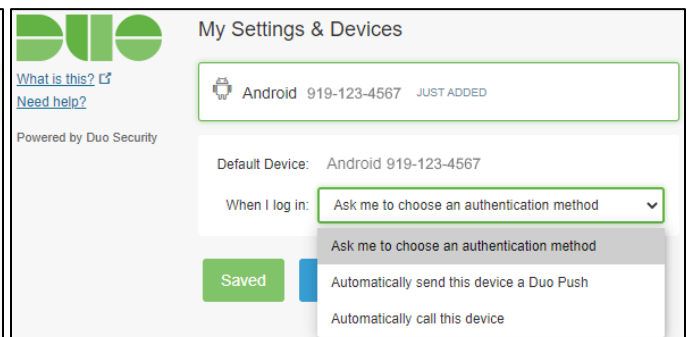
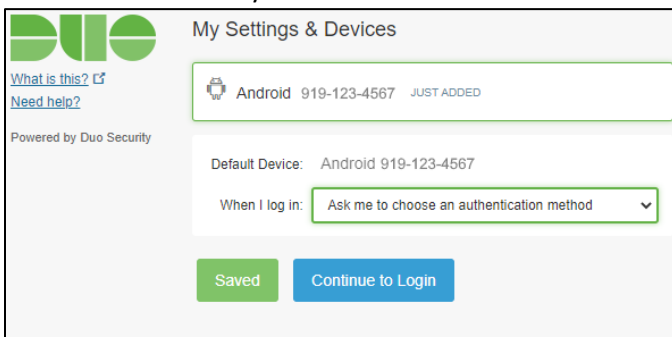


5. Follow the onscreen instructions to activate your Duo Security MFA for use with RENCI SelfService. Click **Continue**.



6. Decide how Duo responds to SelfService logins. Click the **When I log in** dropdown and choose one:

- Ask me to choose an authentication method.
- Automatically send this device a Duo Push
- Automatically call this device





Click **Save** to confirm your preferred method. Then click **Continue to Login**.

## MFA Recovery

You can use backup verification codes if you are unable to prove your identity. Backup Verification Codes help prove your identity if you lose access to your registered MFA device or are unable to prove your identity via the enrolled MFA methods. Each code cannot be used more than once. Once you create a new set of 5 backup codes, the old ones become inactive.

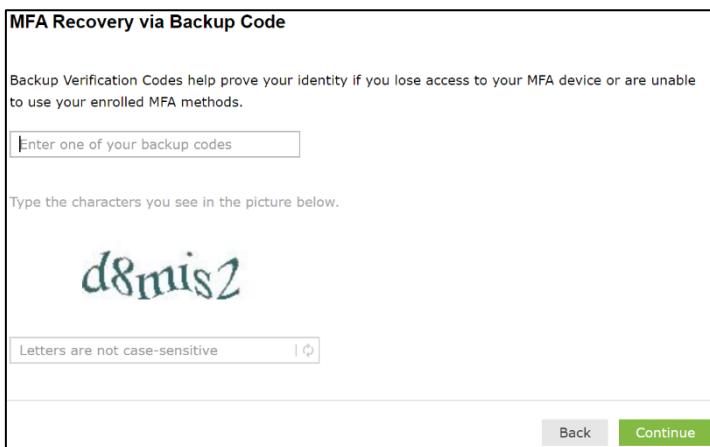
In the RENCIS SelfService portal, go to the **Enrollment** tab → **MFA Recovery** → **Set up**.

When the backup verification codes have been generated, you are given the option to:

- Save as text.
- Send as Email.
- Print

Be mindful to save these codes in a safe place for future use.

To use your backup recover code, login as you normal would. When you get to the verification code page, select **Use backup code**.




**MFA Recovery via Backup Code**

Backup Verification Codes help prove your identity if you lose access to your MFA device or are unable to use your enrolled MFA methods.

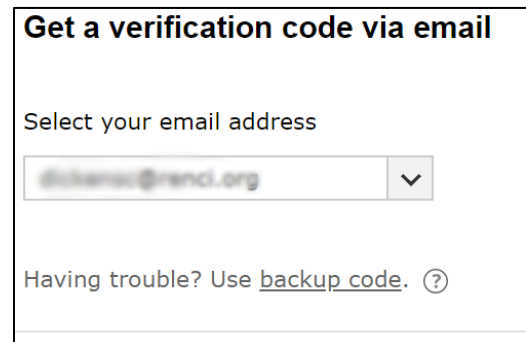
Enter one of your backup codes

Type the characters you see in the picture below.



Letters are not case-sensitive

Back Continue



**Get a verification code via email**

Select your email address

▼

Having trouble? Use [backup code](#). (?)

On the following page, enter a **backup code**, then enter the characters from the **CAPTCHA** image. Click **Continue**.