

2.2 Setup and Usage Procedures for Multi-Factor Authentication

There are multiple methods for multi-factor authentication.

This section explains the setup and usage procedures for the following authentication methods.

Please review the procedures in 2.2.1 through 2.2.4, select the method that best suits your needs, and set up multi-factor authentication.

If you have no specific preference, we recommend setting it up using the Authenticator App as described in section 2.2.1.

2.2.1 Setting Up with Authenticator App

This is the method of receiving a verification code via an authenticator app.

Intended Users

- Users who have no issue installing an authenticator app, such as Google Authenticator or Microsoft Authenticator, on their smartphone.
- Users who already use an authenticator app, such as Google Authenticator or Microsoft Authenticator.

What to Prepare

- Smartphone
- Authenticator app
e.g., Google Authenticator, Microsoft Authenticator, Authy, etc.

Setup Procedure (This example uses Google Authenticator.)

1. Download and install an authenticator app from the App Store or Google Play.

Note: If you have already installed an app, please proceed to Step 2.



iOS,iPadOS : Google Authenticator

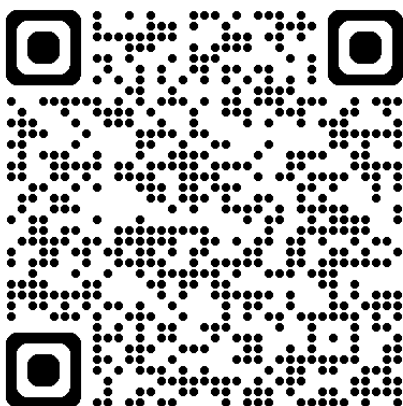
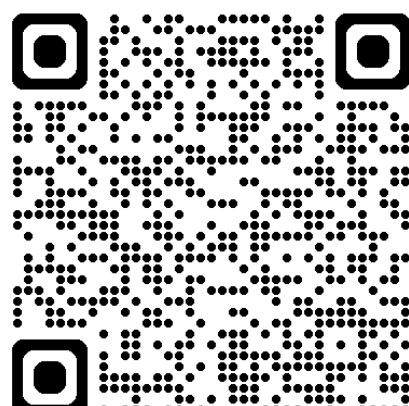
Android : Google Authenticator



App Store



Google Play



2.2.1 Setting Up with Authenticator App

2. Complete "2.1 Preparing for Multi-Factor Authentication" and open the 2-Step Verification screen.
3. Select "Authenticator".

← 2-Step Verification

Turn on 2-Step Verification

Prevent hackers from accessing your account with an additional layer of security.

Unless you're signing in with a passkey, you'll be asked to complete the most secure second step available on your account. You can update your second steps and sign-in options any time in your settings. [Go to Security Settings](#)



Second steps

Make sure you can access your Google Account by keeping this information up to date and adding more sign-in options

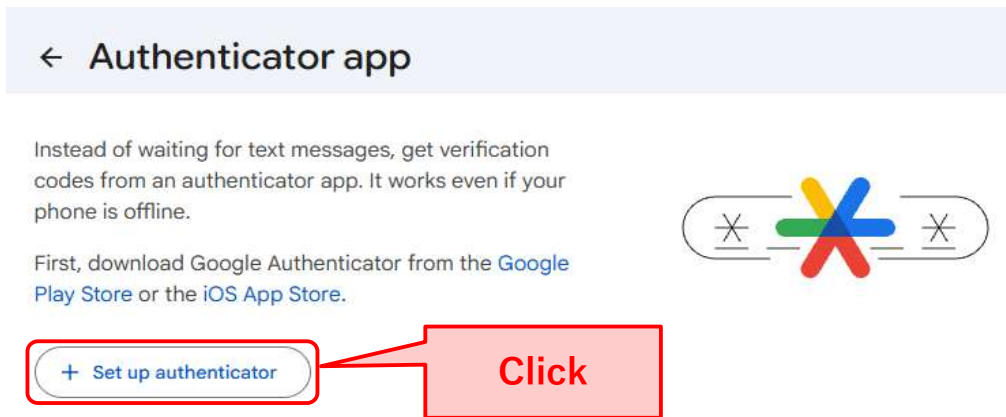
- | | | | |
|---|----------------------------|---|---|
|  | Passkeys and security keys |  Add a passkey | + |
|  | Google prompt | | > |
|  | Authenticator |  Add authenticator app | > |
|  | Phone number |  Add a phone number | > |

Click

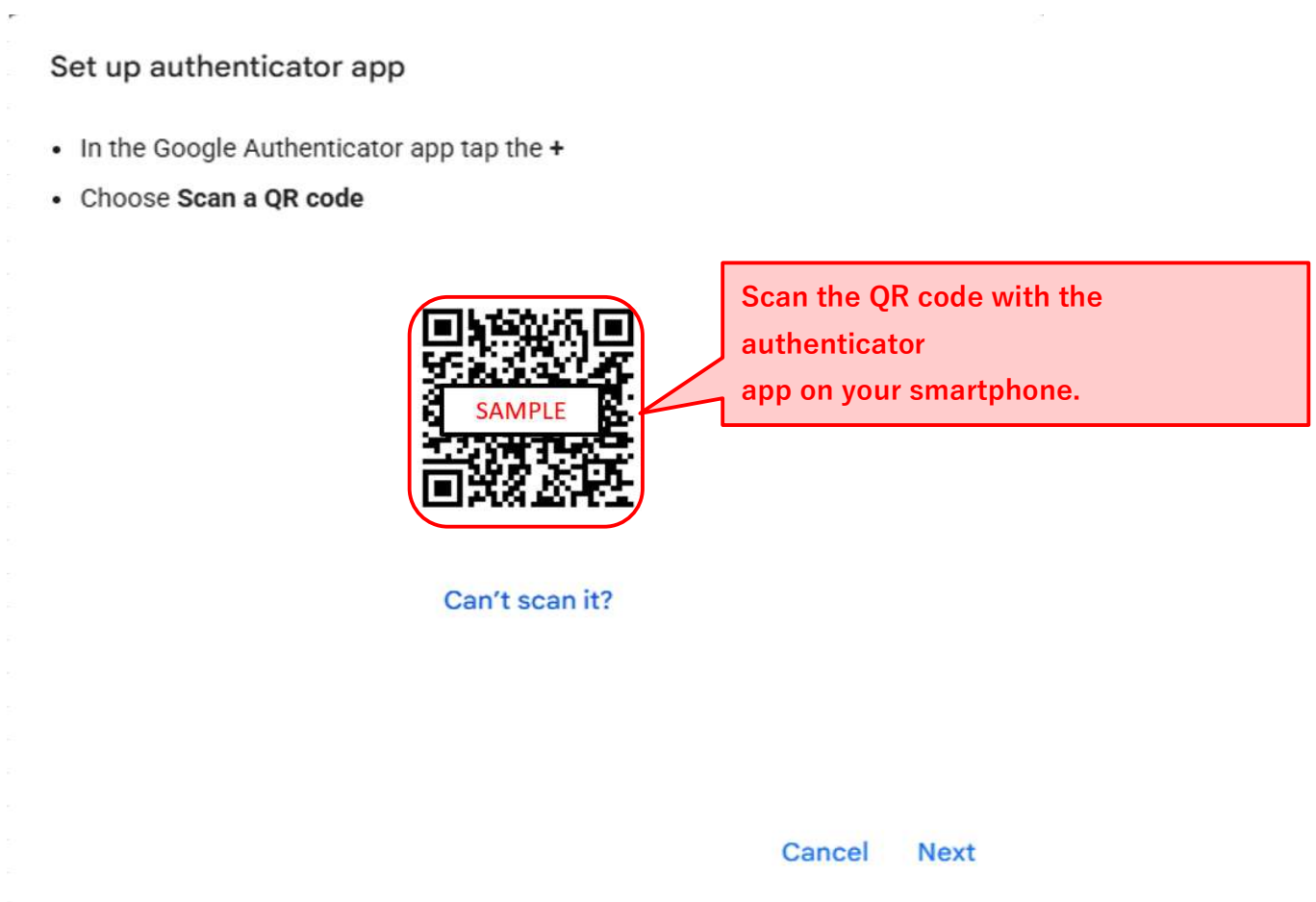
Turn on 2-Step Verification

2.2.1 Setting Up with Authenticator App

4. Select "+ Set up authenticator".

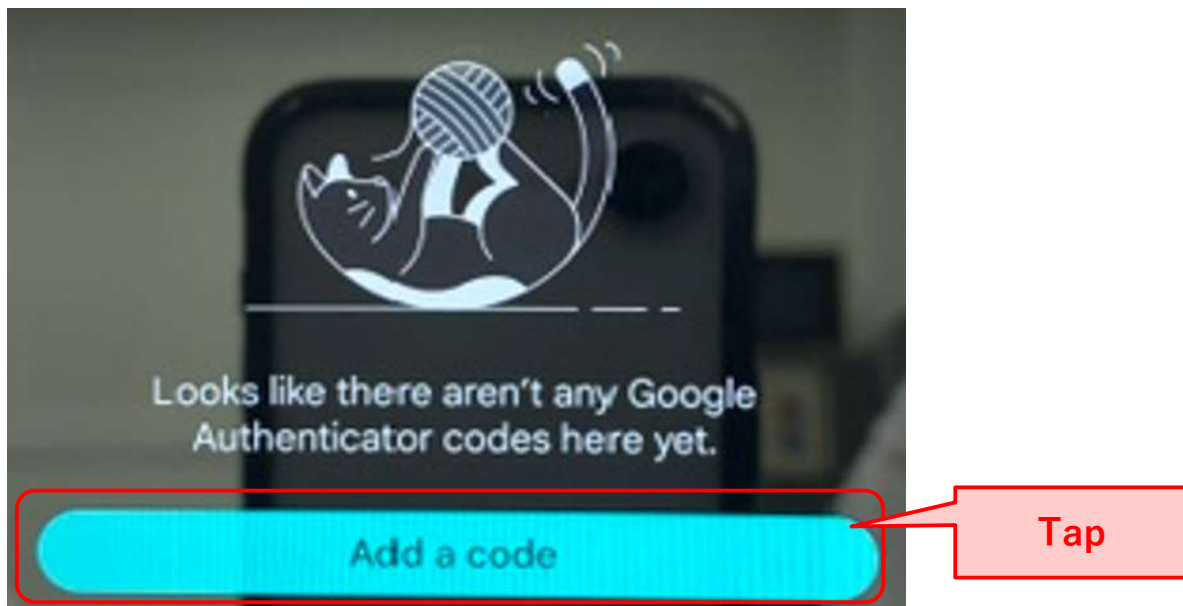


5. A QR code will appear on the screen.

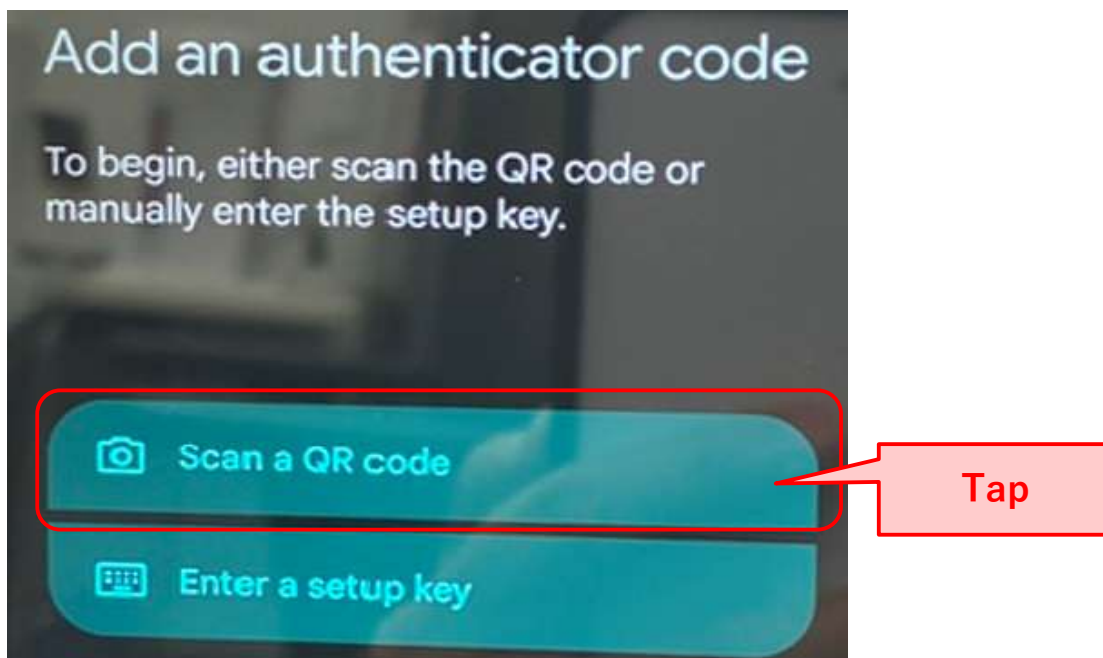


2.2.1 Setting Up with Authenticator App

6. Open the authenticator app and tap "Add a code".

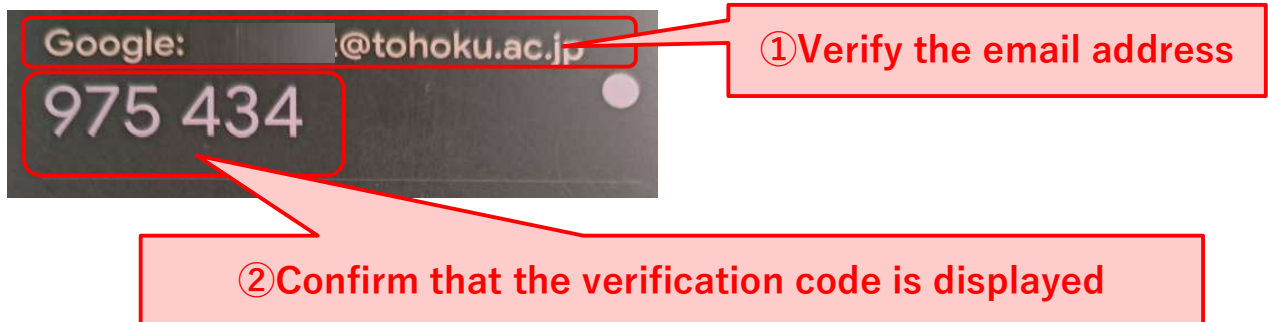


7. Tap "Scan a QR code".

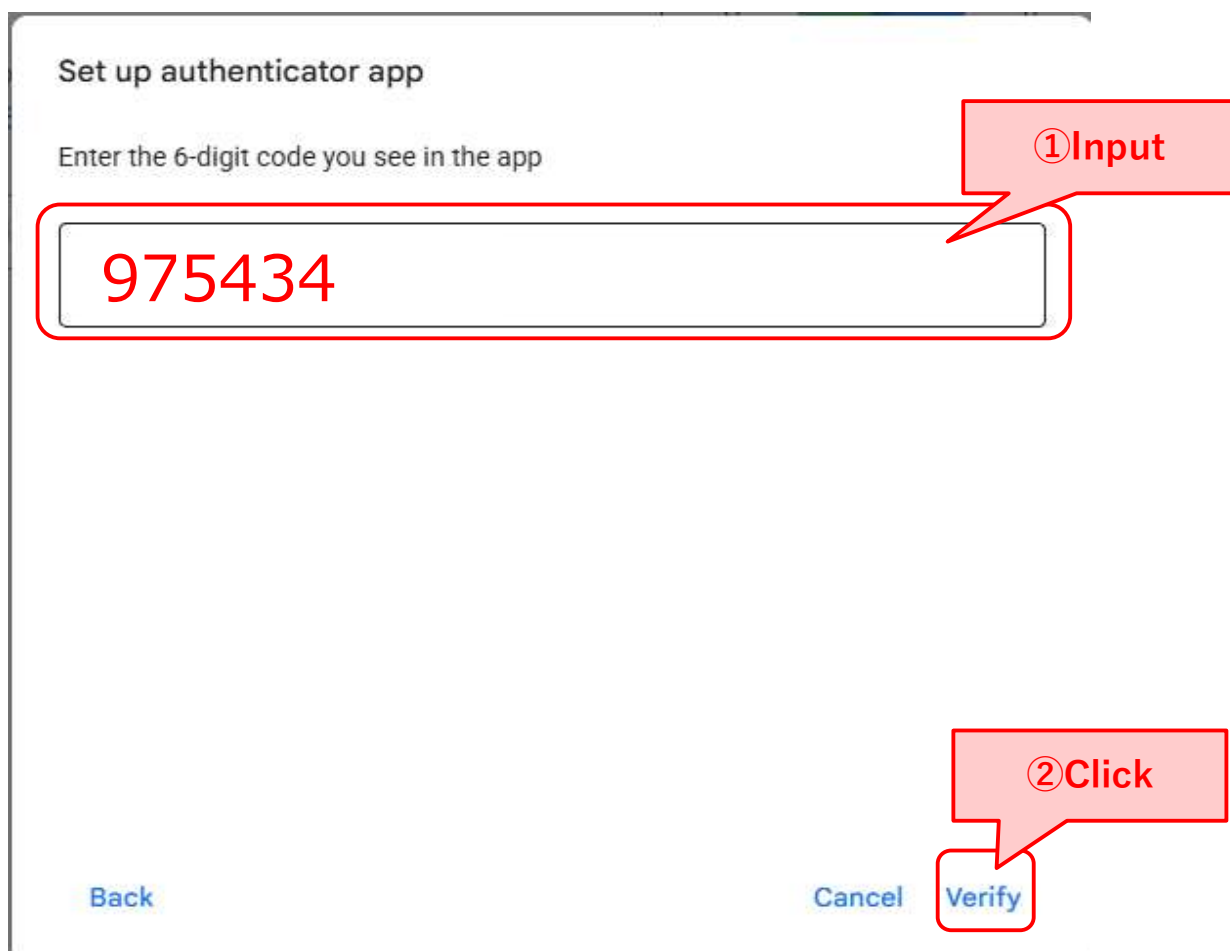


2.2.1 Setting Up with Authenticator App

8. The authenticator app will be set up, and a verification code will be displayed.
Please check if your Tohoku University email address is displayed.

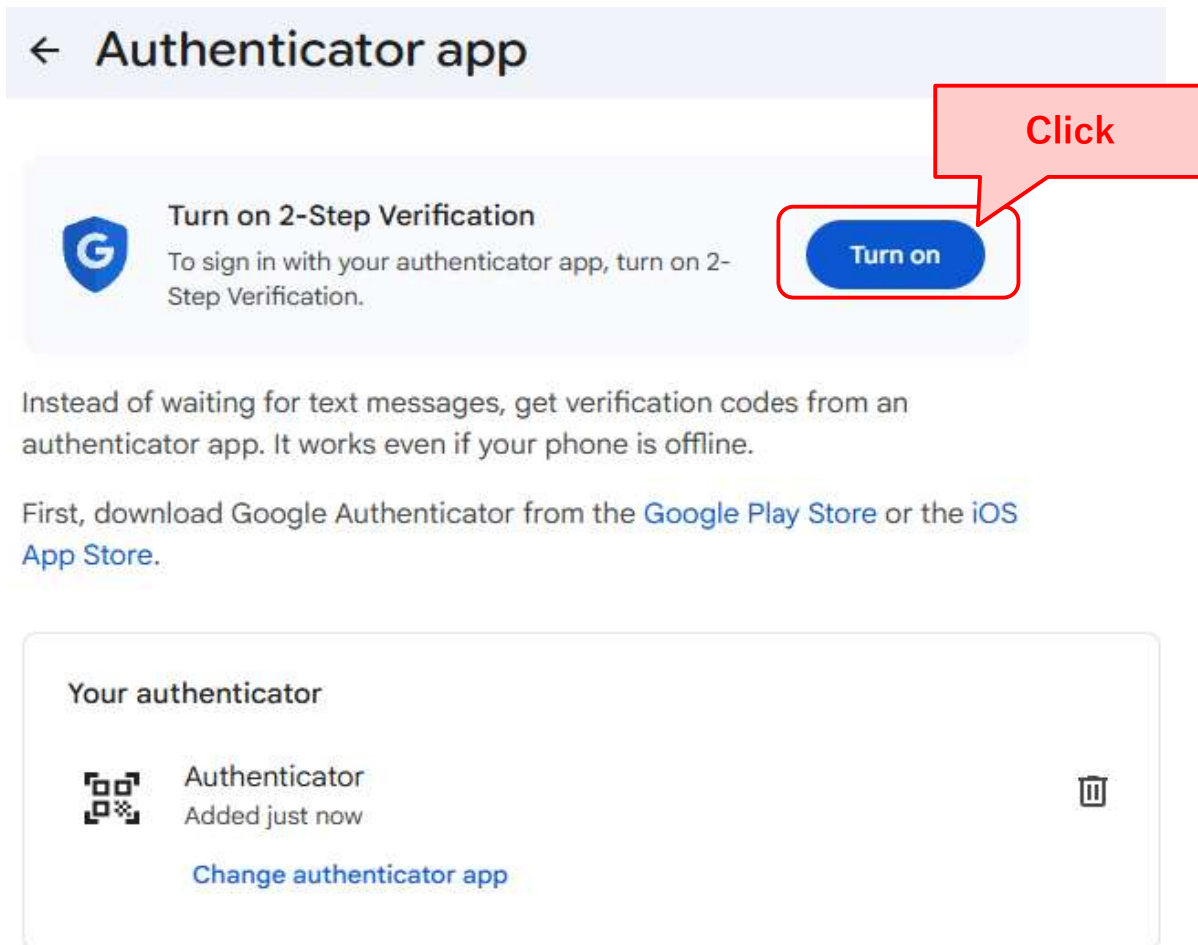


9. Enter the 6-digit code displayed on your authenticator app onto your computer screen.
10. Select "Verify".



2.2.1 Setting Up with Authenticator App

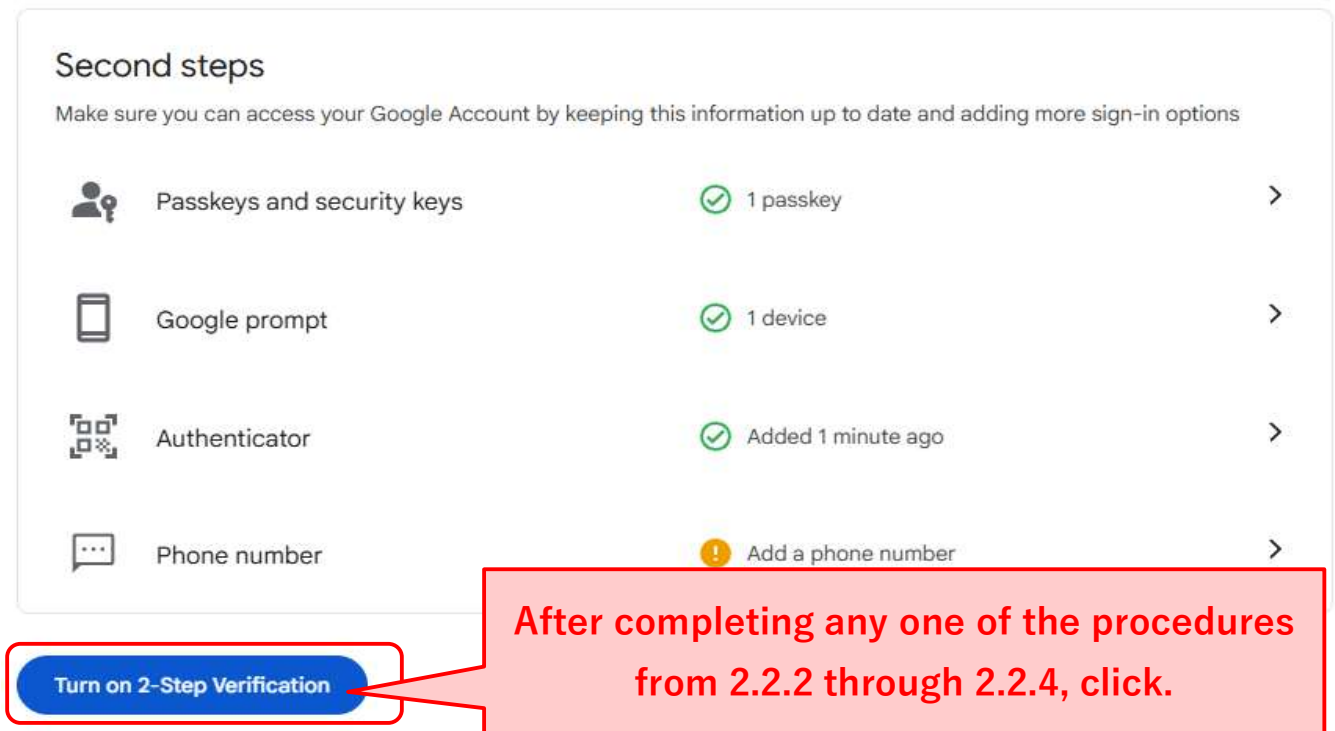
11. Select "Turn on".



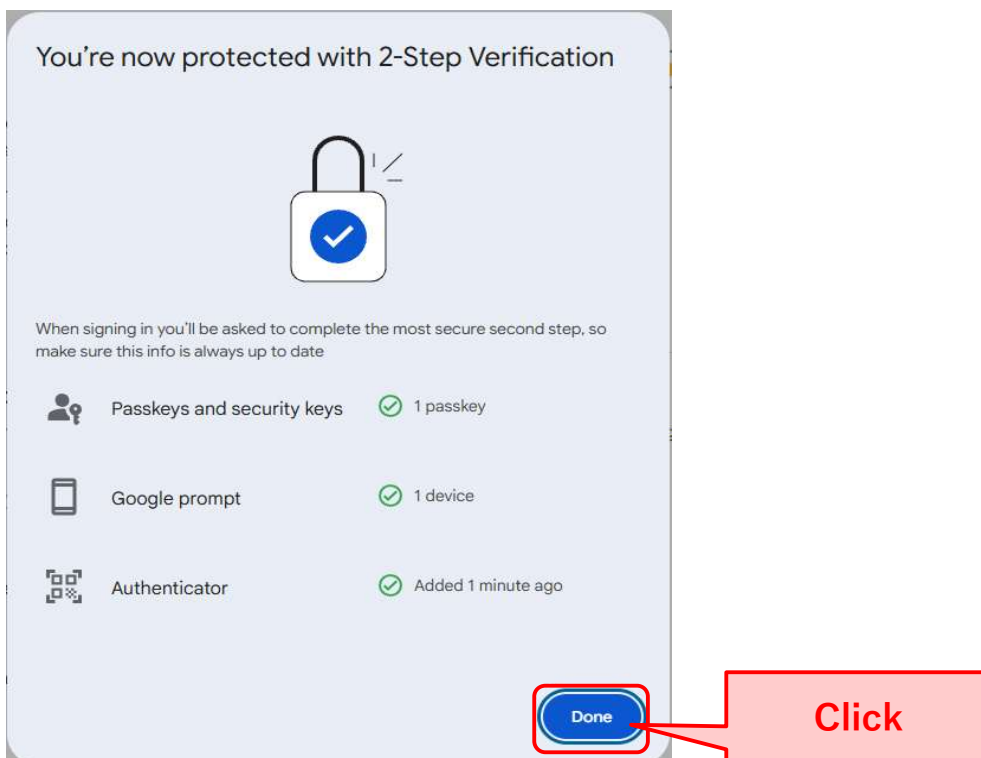
2.2.1 Setting Up with Authenticator App

12. Select "Turn on 2-Step Verification".

Regarding 2-Step Verification, in addition to this procedure, please also complete any one of the procedures from 2.2.2 through 2.2.4.

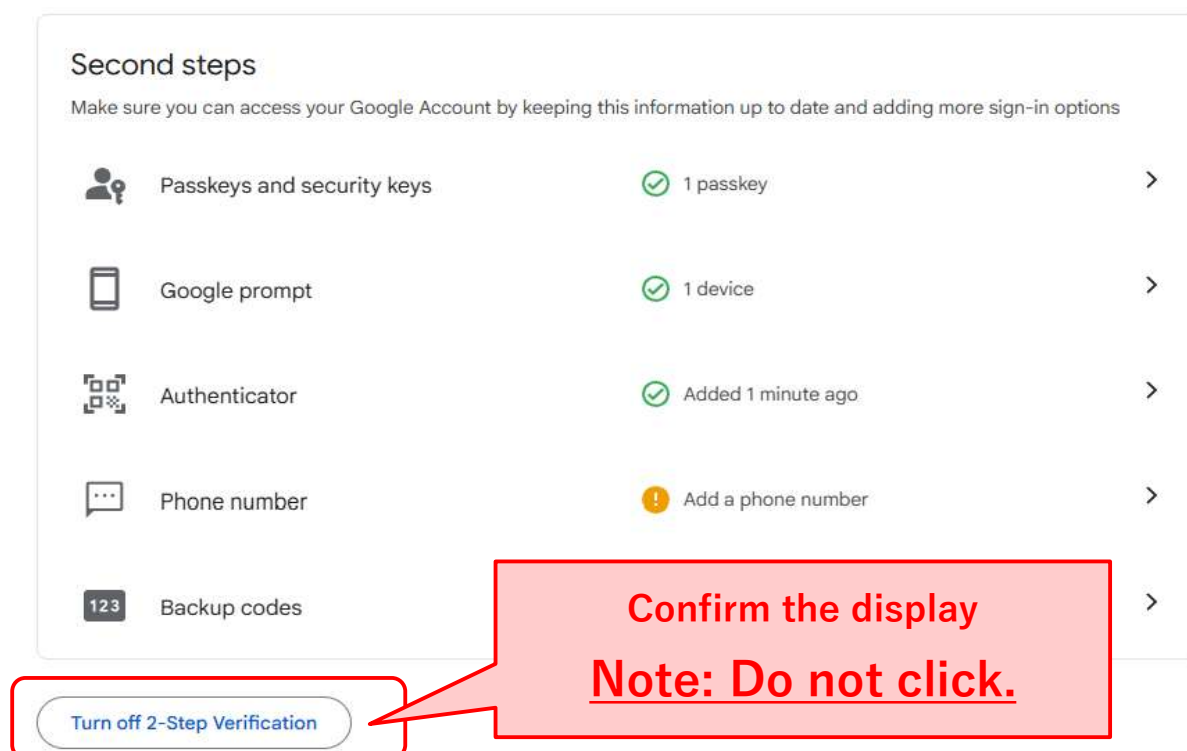


13. Select "Done".



2.2.1 Setting Up with Authenticator App

14. Confirm that "Turn off 2-Step Verification" is displayed.



If "Turn off 2-Step Verification" is not displayed, the setup is not complete. Please check the steps again.

This completes the setup for "2.2.1 Setting Up with Authenticator App".

For instructions on how to log in using the authenticator app, please see the following pages.

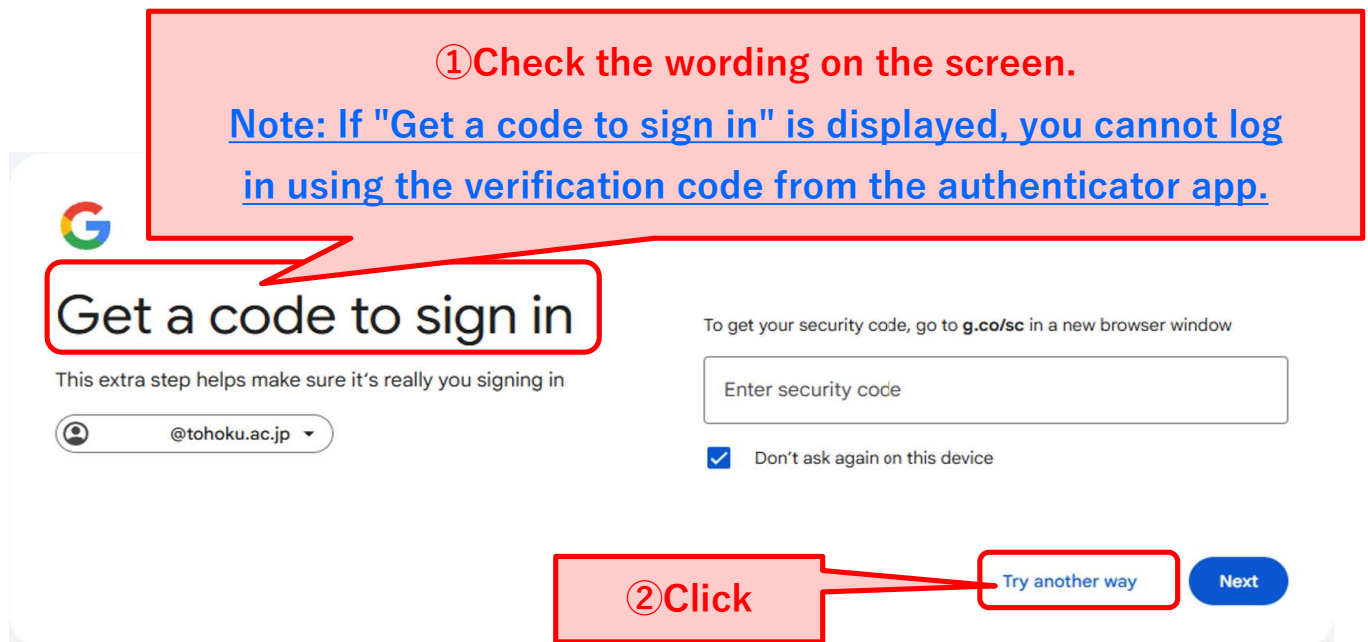
In addition, please be sure to complete "2.2.5 Setting Up Backup Codes" to prepare for unexpected circumstances.

<https://www.bureau.tohoku.ac.jp/i-synergy/tumail/manual/2-2-5-eng.pdf>

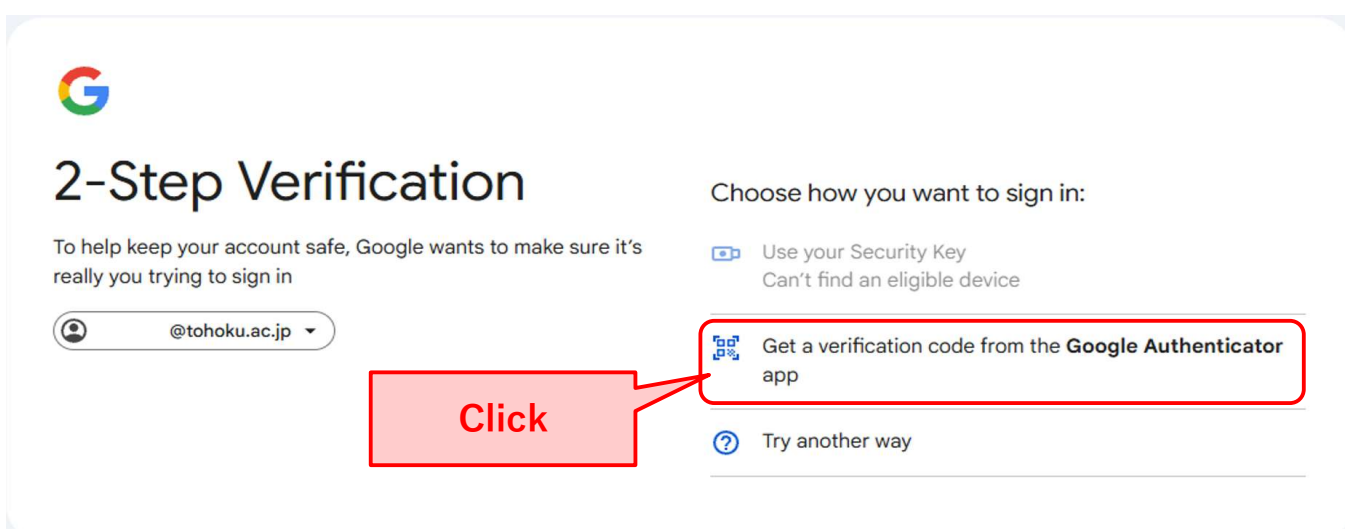
2.2.1 Setting Up with Authenticator App

Usage Procedures

1. Enter your email address and password on the Google login screen.
2. If the "Get a code to sign in" screen appears, select "Try another way".

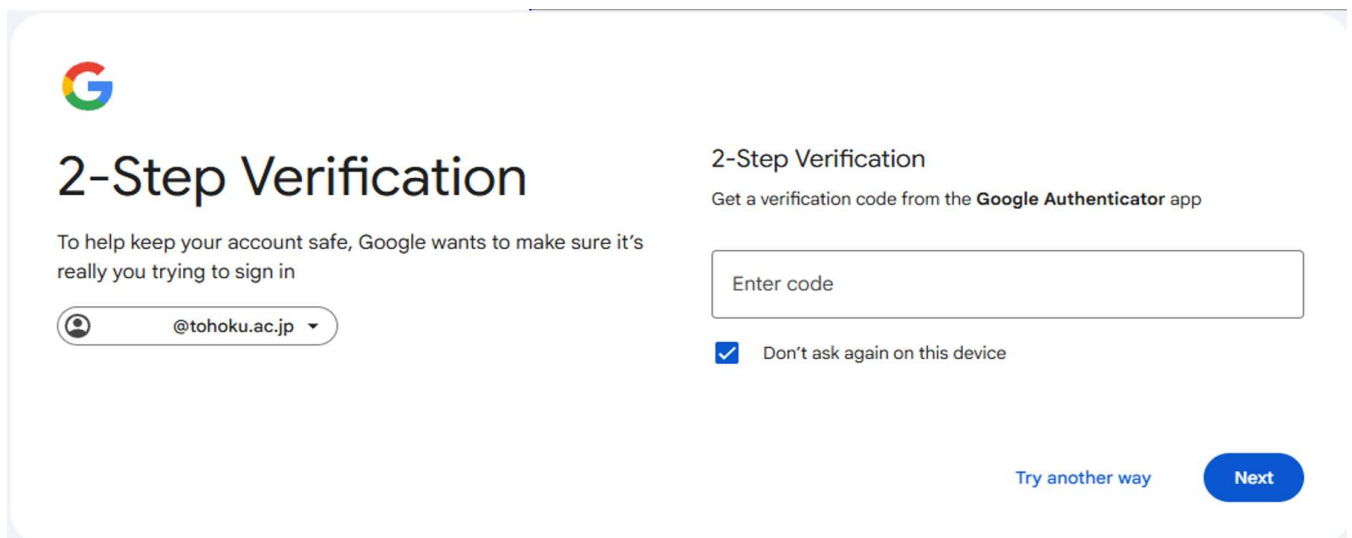


3. If you are prompted for a login method, select "Get a verification code from the Google Authenticator app".



2.2.1 Setting Up with Authenticator App

4. When logging in, "2-Step Verification" will appear.

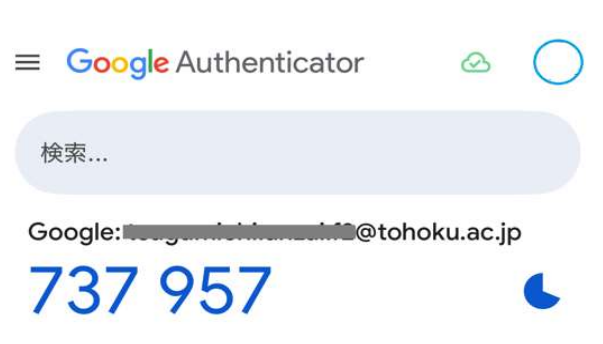


5. Open the authenticator app and check the verification code.

< Android >



< iPhone >



2.2.1 Setting Up with Authenticator App

6. Enter the "security code" and select "Next".

Note: If you are using a shared computer or a computer that is not exclusively yours, please uncheck the box for "Don't ask again on this device."

The screenshot shows the Google 2-Step Verification interface. The Google logo is at the top left. Below it, the title "2-Step Verification" is displayed. A message states: "To help keep your account safe, Google wants to make sure it's really you trying to sign in". Below this message is a dropdown menu showing "@tohoku.ac.jp". To the right, the text "2-Step Verification" is followed by "Get a verification code from the Google Authenticator". A text input field contains the code "975434". Below the input field is a checkbox labeled "Don't ask again on this device", which is currently checked. At the bottom right, there is a "Try another way" link and a blue "Next" button. Red annotations are present: a box labeled "① Input" points to the verification code input field; a box labeled "② Uncheck as necessary" points to the "Don't ask again on this device" checkbox; and a box labeled "③ Click" points to the "Next" button.

7. Login is complete.

Next, please be sure to complete "2.2.5 Setting Up Backup Codes".

<https://www.bureau.tohoku.ac.jp/i-synergy/tumail/manual/2-2-5-eng.pdf>