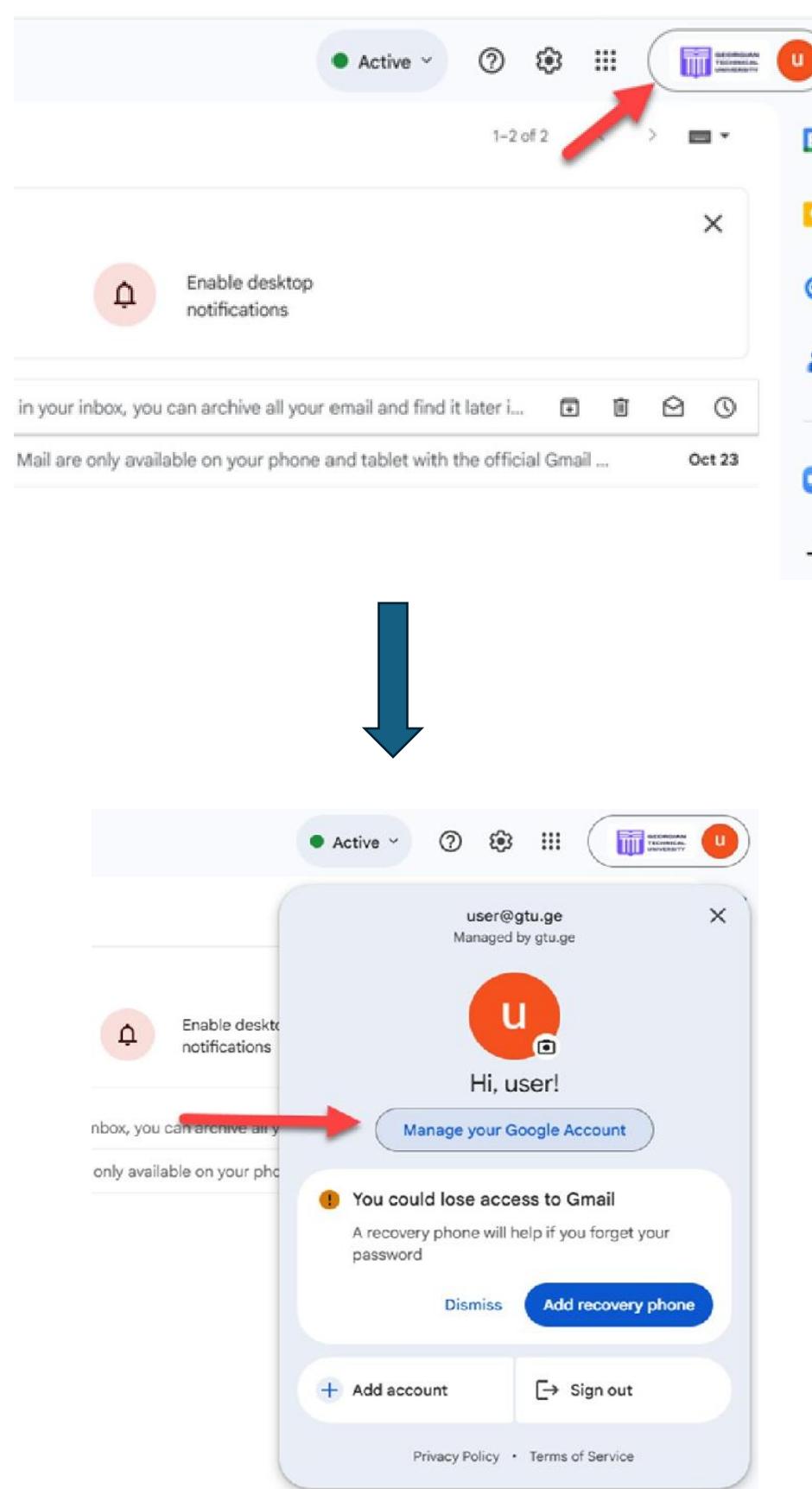




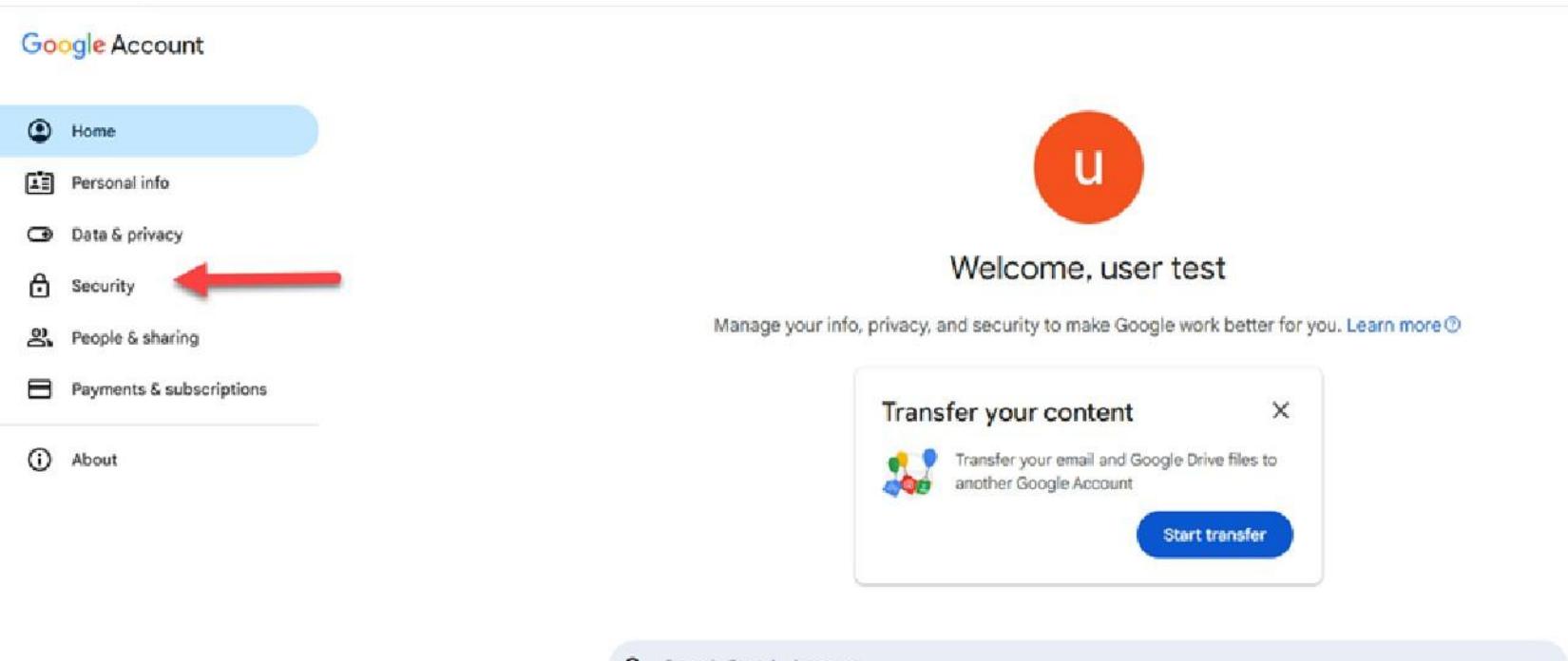
სტუ-ს ელექტრონულ ფოსტაზე (e-mail) ორმაგი ავთენტიფიკაციის ჩართვის ინსტრუქცია

ნაბიჯი 1:

1.1. mail.gtu.ge ან www.gmail.com-ზე მომხმარებლის პარამეტრებით(მომხმარებლის სახელი და პაროლი) შესვლის შემდეგ, გადადით თქვენი Google ანგარიშის უსაფრთხოების პარამეტრებზე. Gmail-ის ზედა მარჯვენა კუთხეში დაწვაპუნებით თქვენი პროფილის ხატულაზე. შემდეგ აირჩიეთ Google ანგარიშის მართვა - [Manage Your Google Account](#).



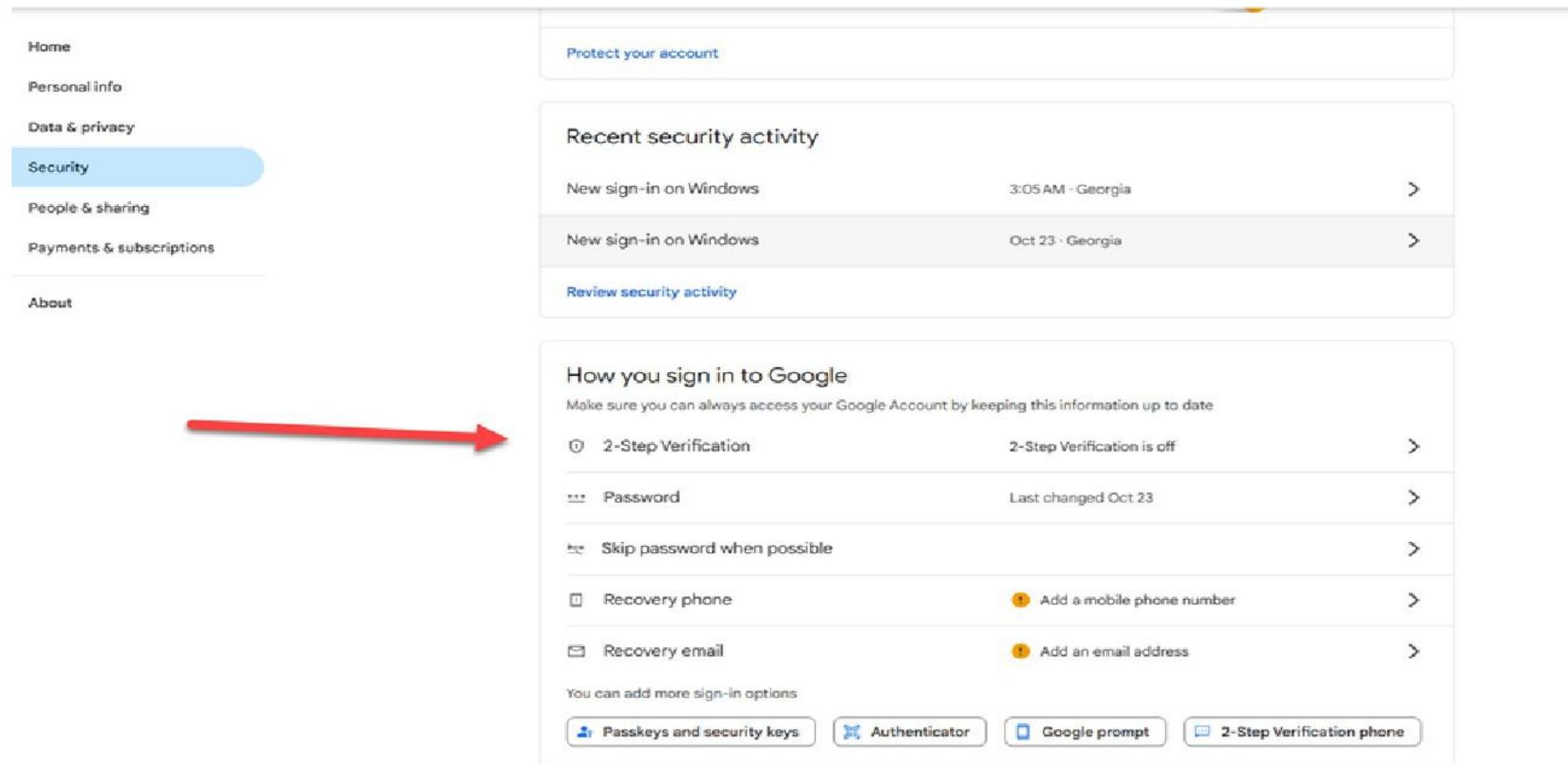
1.2. მარცხენა ნავიგაციის პანელში დააწვაპუნეთ **Security** (უსაფრთხოების) ღილაკზე.



ნაბიჯი 2:

2.1. დაიწყეთ 2-ეტაპიანი ავთენტიფიკაციის დაყენება

- გადადით [How you sign in to Google](#) განყოფილებაში
- დააჭირეთ [2-Step Verification](#) ღილაკს და დააწვაპუნეთ [Get started.](#)



Home
Personal info
Data & privacy
Security
People & sharing
Payments & subscriptions
About

Protect your account

Recent security activity

New sign-in on Windows 3:05 AM - Georgia >

New sign-in on Windows Oct 23 - Georgia >

Review security activity

How you sign in to Google

Make sure you can always access your Google Account by keeping this information up to date

2-Step Verification 2-Step Verification is off >

>Password Last changed Oct 23 >

Skip password when possible >

Recovery phone Add a mobile phone number >

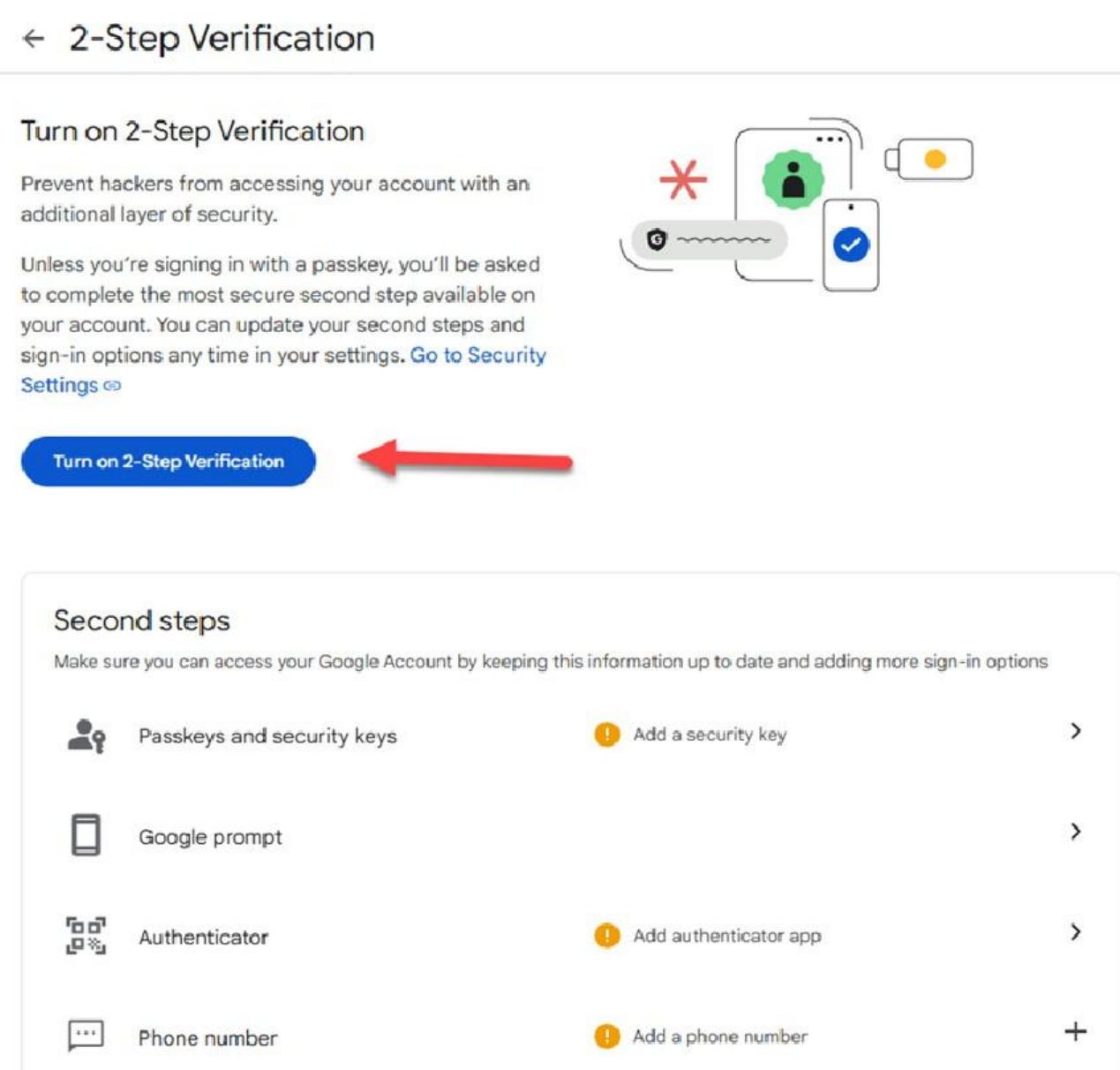
Recovery email Add an email address >

You can add more sign-in options

Passkeys and security keys Authenticator Google prompt 2-Step Verification phone

ნაბიჯი 3:

3.1 დააჭირეთ ღილაკს [Turn on 2-Step Verification](#)



← 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](#)

Turn on 2-Step Verification ←

Second steps

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

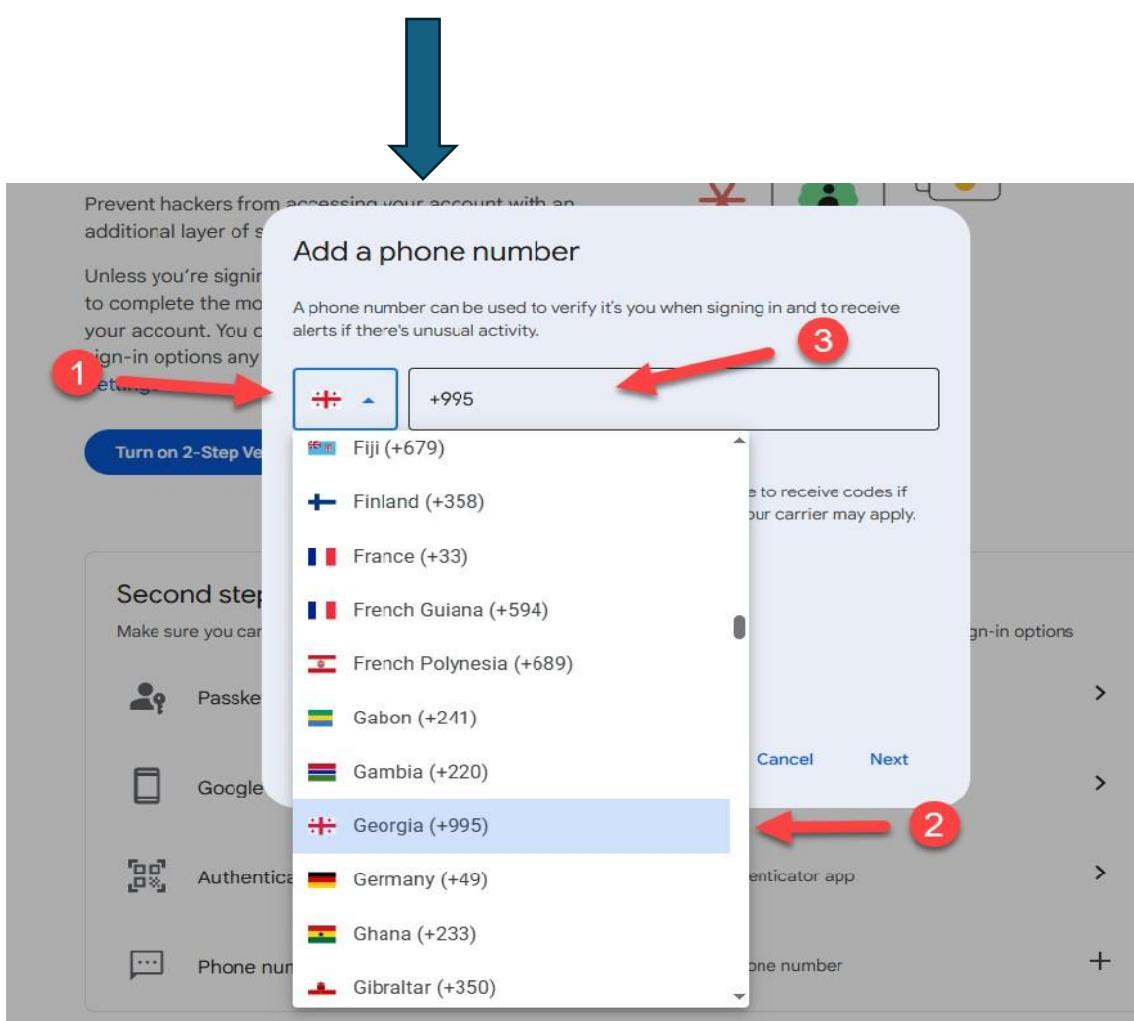
Passkeys and security keys Add a security key >

Google prompt >

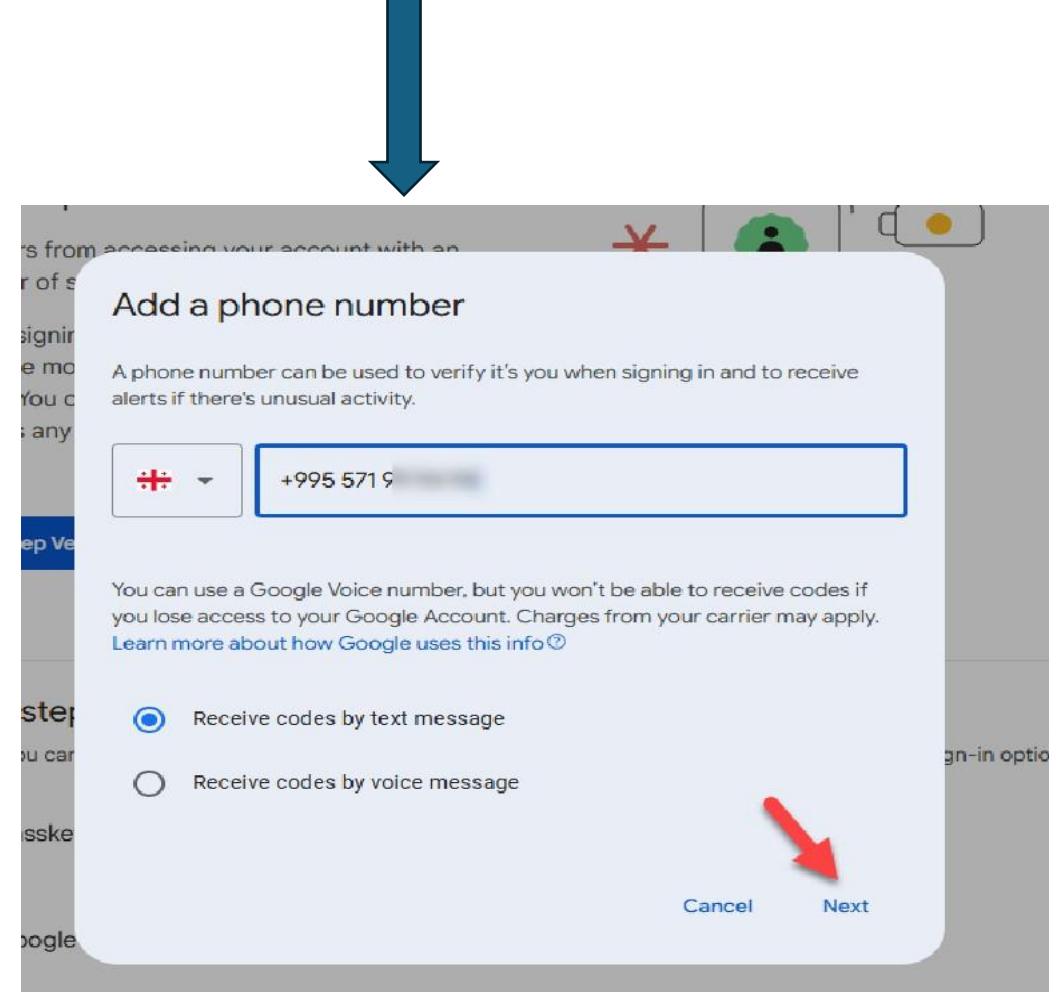
Authenticator Add authenticator app >

Phone number Add a phone number +

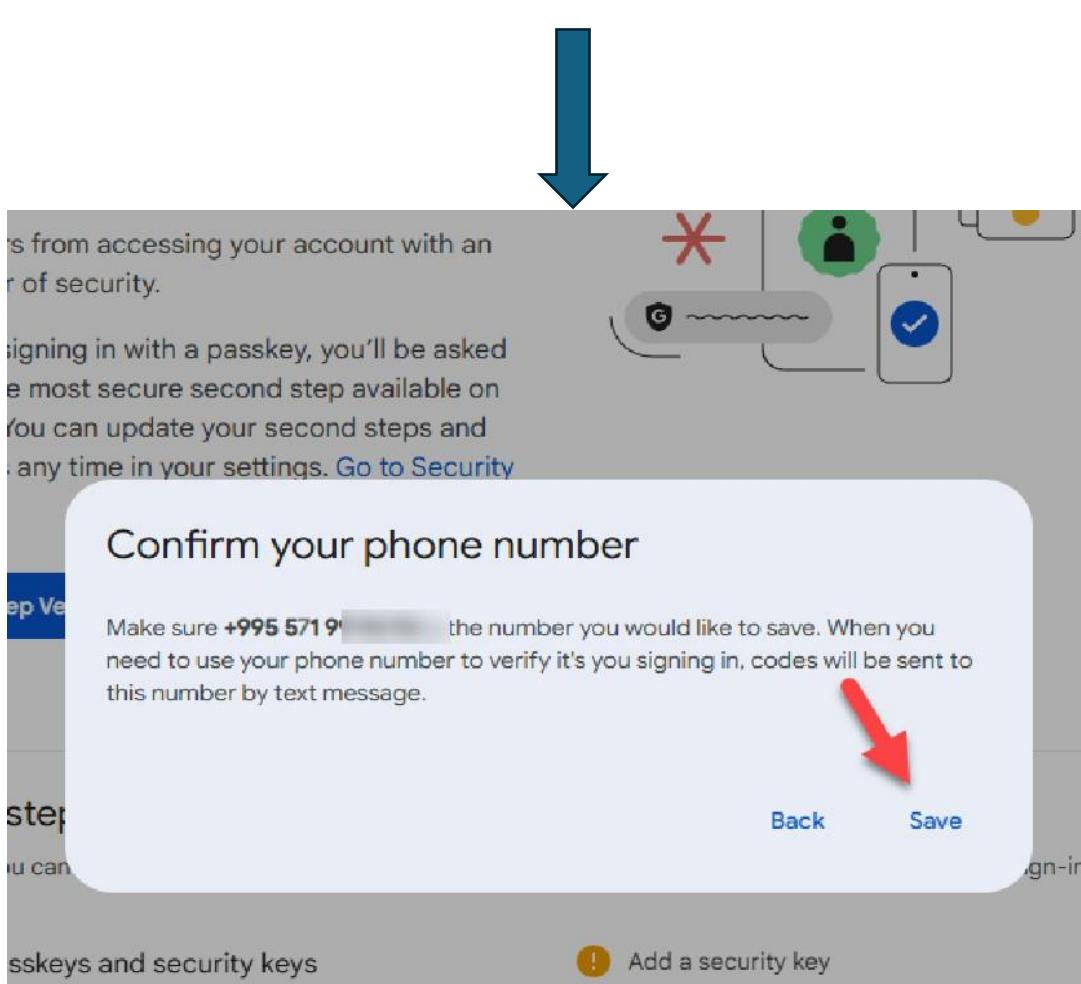
3.2 ჩამონათვალში აირჩიეთ საქართველოს ქვეყნის კოდი **Georgia (+995)** და ჩაწერეთ თქვენი მობილურის ნომერი.



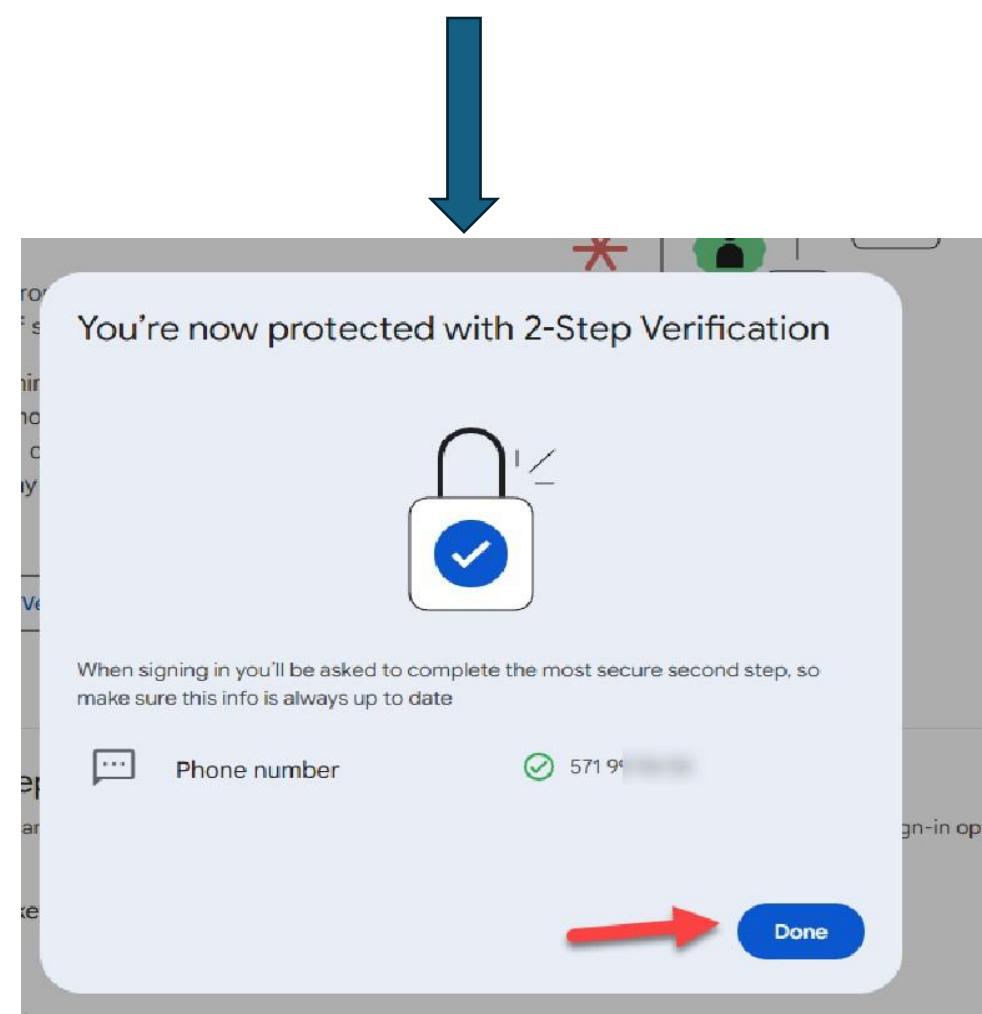
3.3 მობილურის ნომრის ჩაწერის შემდეგ დააჭირეთ **Next** ღილაკს.



3.4 შეტყობინება **Confirm your phone number** გამოსვლის შემდეგ დააჭირეთ **Save** ღილაკს.

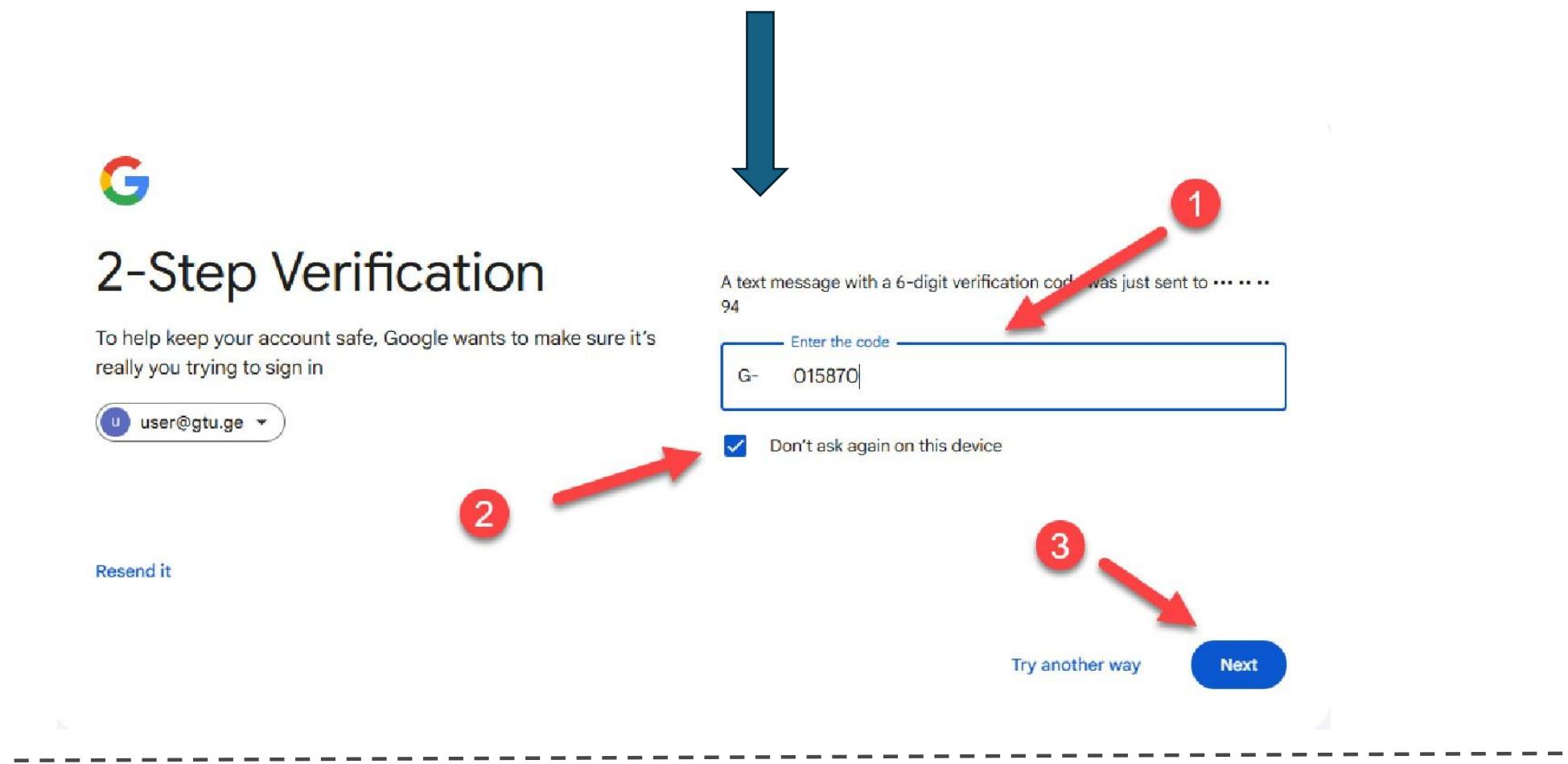


3.5 თქვენ გაგიაქტიურდათ 2-ფაქტორიანი ავთენტიფიკაცია, დააჭირეთ ღილაკს **Done**.



ელექტრონულ ფოსტაზე ხელმეორედ შესვლის შემდეგ, მითითებულ მობილურ ნომერზე გამოიგზავნება SMS-ის 6 ციფრიანი კოდი. თუ გსურთ გარკვეული პერიოდის განმავლობაში აღარ მოგთხოვთ კოდის ხელახლა ჩაწერა, მონიშნეთ ველი **Don't ask again on this device**. და დააჭირეთ ღილაკს **Next**.

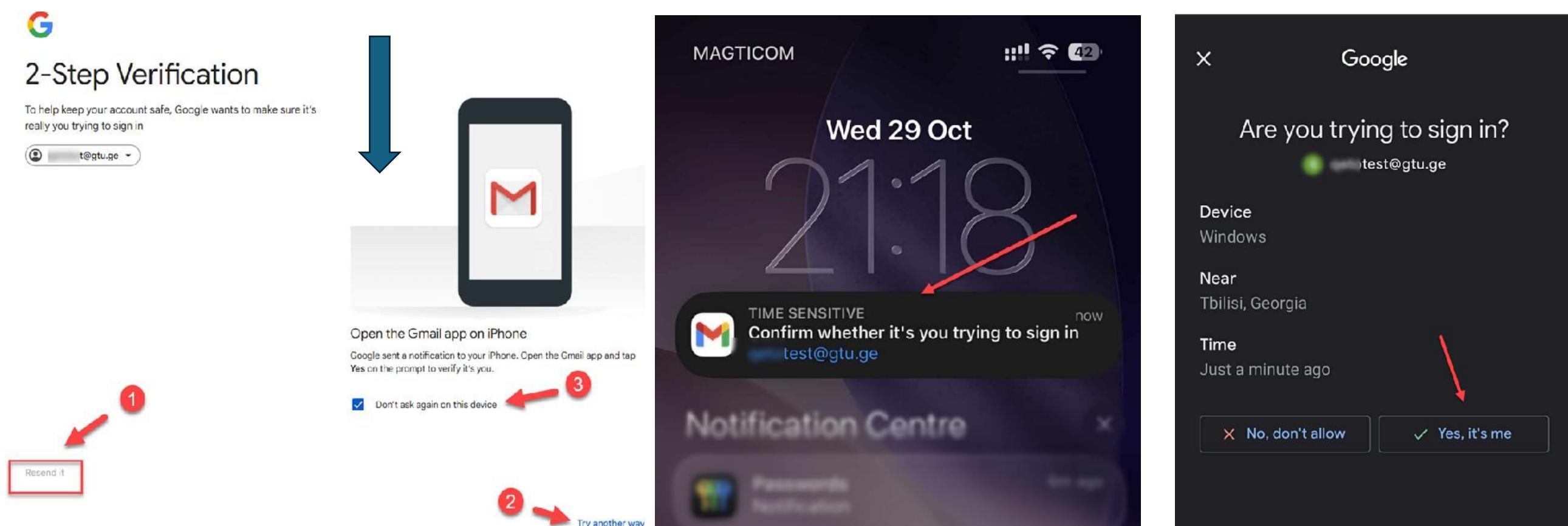
ამის შემდეგ, ელ.ფოსტა გაიხსნება და მოწყობილობა ჩაითვლება სანდოდ.



თუ მობილურზე დამატებული გაქვთ ელ. ფოსტა

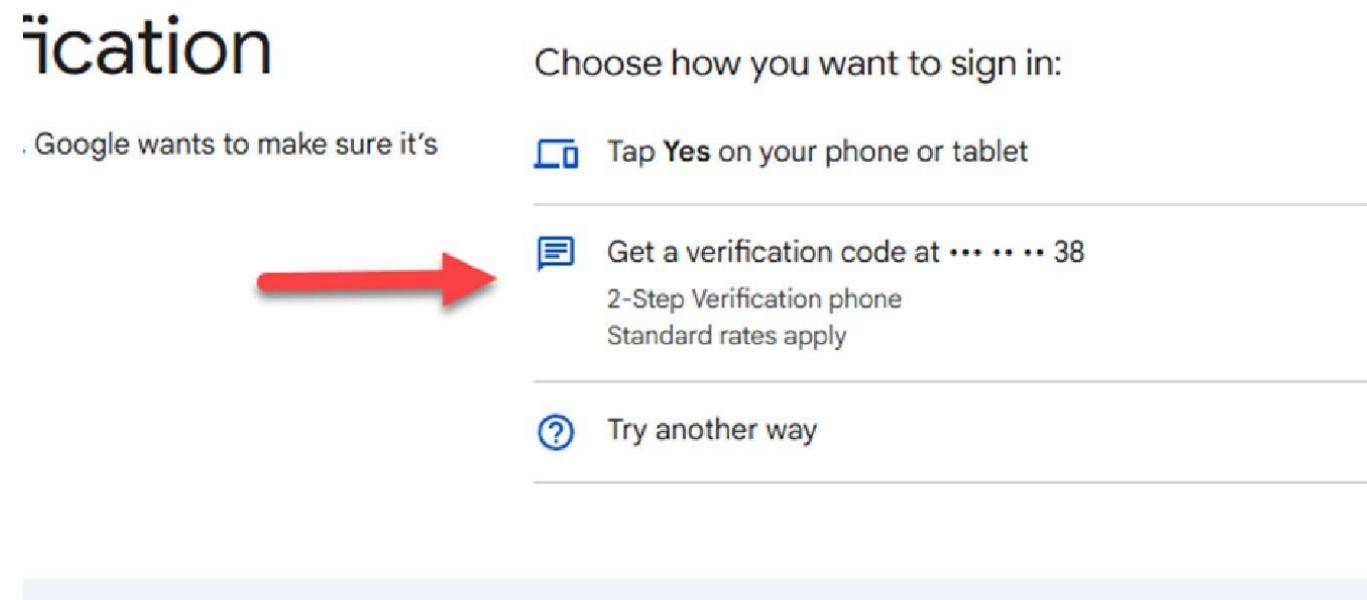
ხელმეორედ შესვლის შემდეგ **Google SMS-ის** გამოგზავნის ნაცვლად, თავდაპირველად მოგთხოვთ მობილურით ავთენტიფიკაციას:

- 1) თუ შეტყობინება ვერ მიიღეთ, შეგიძლიათ დააჭიროთ **Resend it** ღილაკს და ხელმეორედ გამოიგზავნება.
- 2) თუ ამ მეთოდით ვერ გაააქტიურებთ, შეგიძლიათ დააჭიროთ **Try another way** ღილაკს, მიუთითოთ მობილურის ნომერი და გამოგეგზავნებათ ახალი **SMS** შეტყობინება.

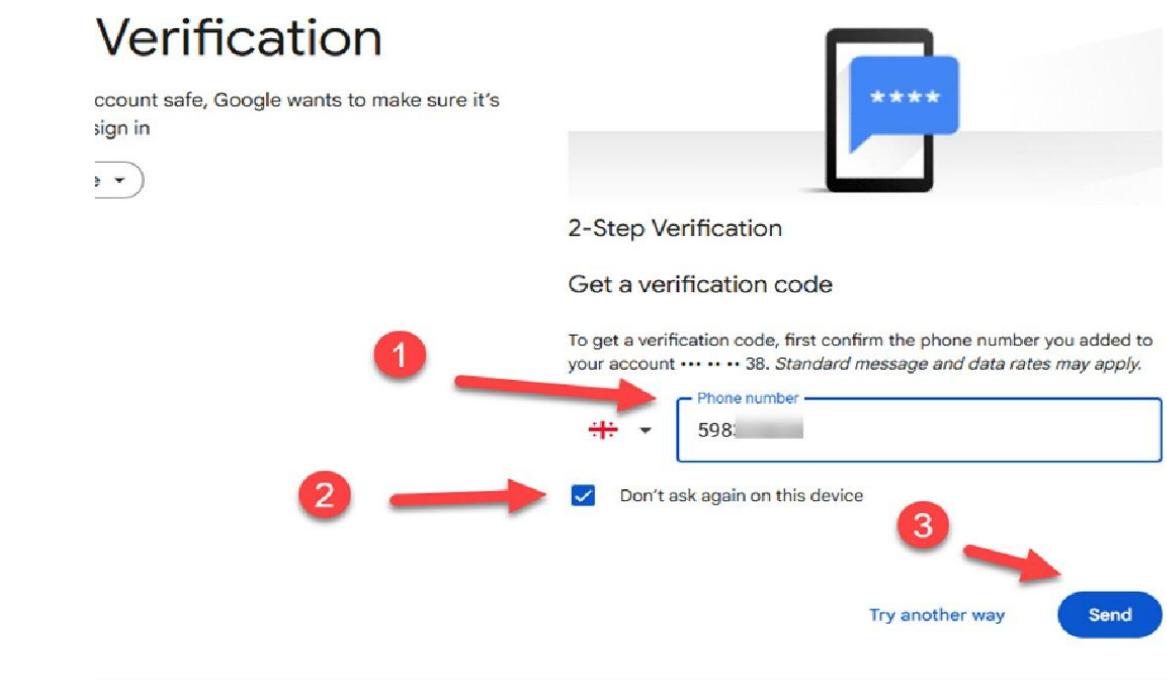


3) მობილურის ნომრის მითითება

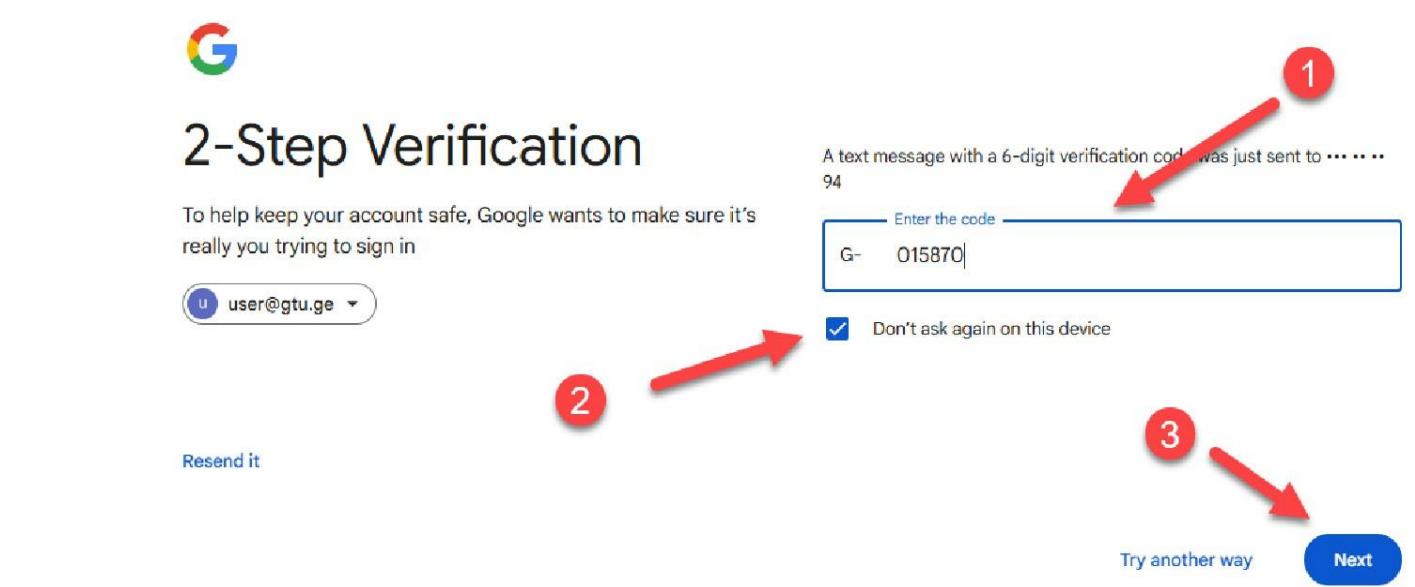
1. აირჩიეთ [Get a verification code](#), სადაც მითითებული მობილურის ნომრის ბოლო 2 ციფრი იქნება ნაჩვენები



2. მიუთითეთ იგივე მობილურის ნომერი



3. მობილურზე გადამოწმეთ [Google](#)-საგან გამოგზავნილი [SMS](#) და მიუთითეთ კოდი



4. [Next](#) ღილაკზე დაჭრის შემდეგ შეხვალთ ელ.ფოსტაში.

გისურვებთ წარმატებას!