Google Authenticator adds 'formidable' security layer to email accounts

Google Authenticator is a free security application that helps protect your account from password theft. This application is extremely easy to set up and can be used during two-factor authentication (2FA) provided on popular services like Gmail, Facebook, Twitter, Instagram, ...

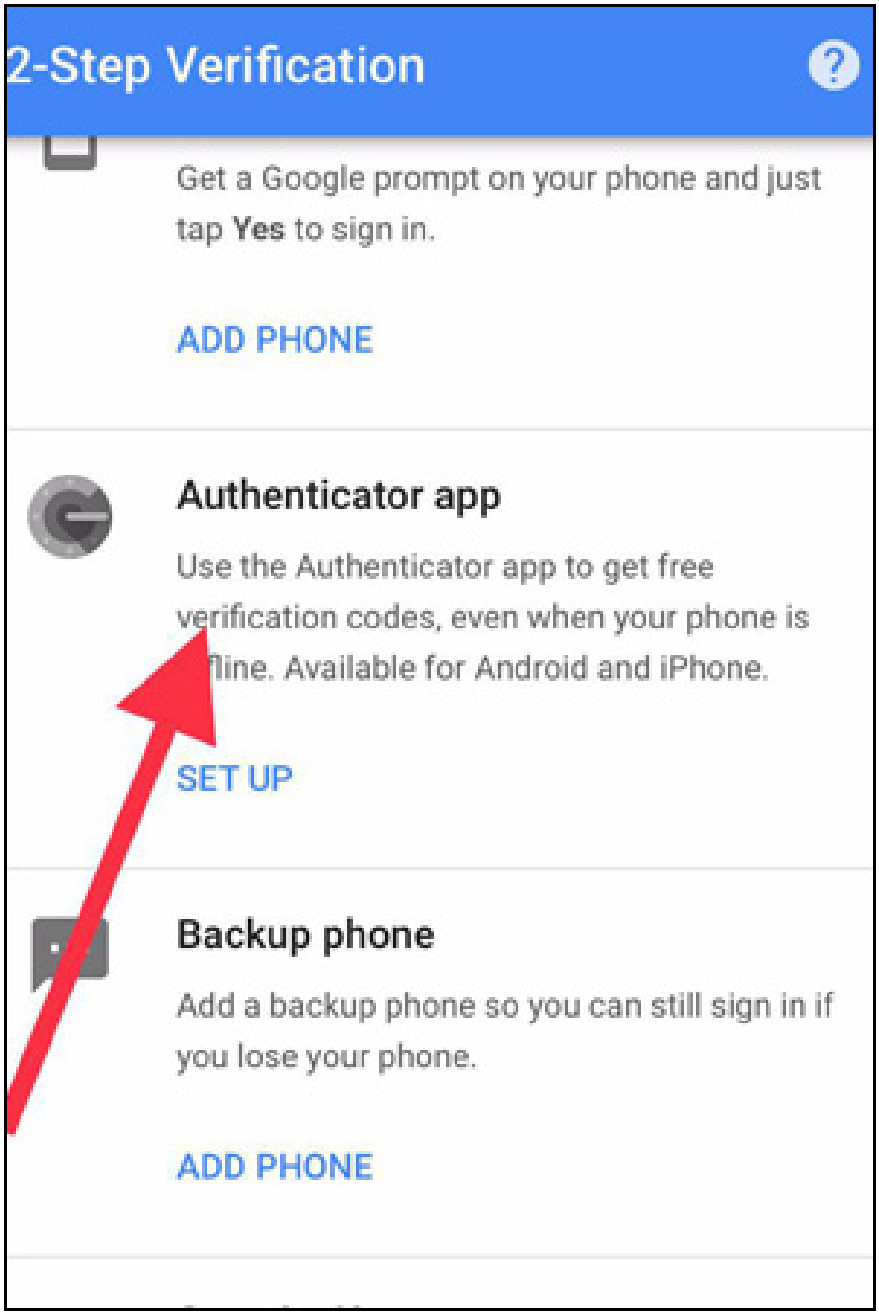
Google Authenticator is a free security application that helps protect your account from password theft. This application is extremely easy to set up and can be used during two-factor authentication (2FA) provided on popular services like Gmail, Facebook, Twitter, Instagram, .

2-factor authentication code (on iOS and Android) will generate a random code to verify your identity when logging into different online services. This code can be sent to your phone via text message at any time - but Google Authenticator will provide a higher level of security.

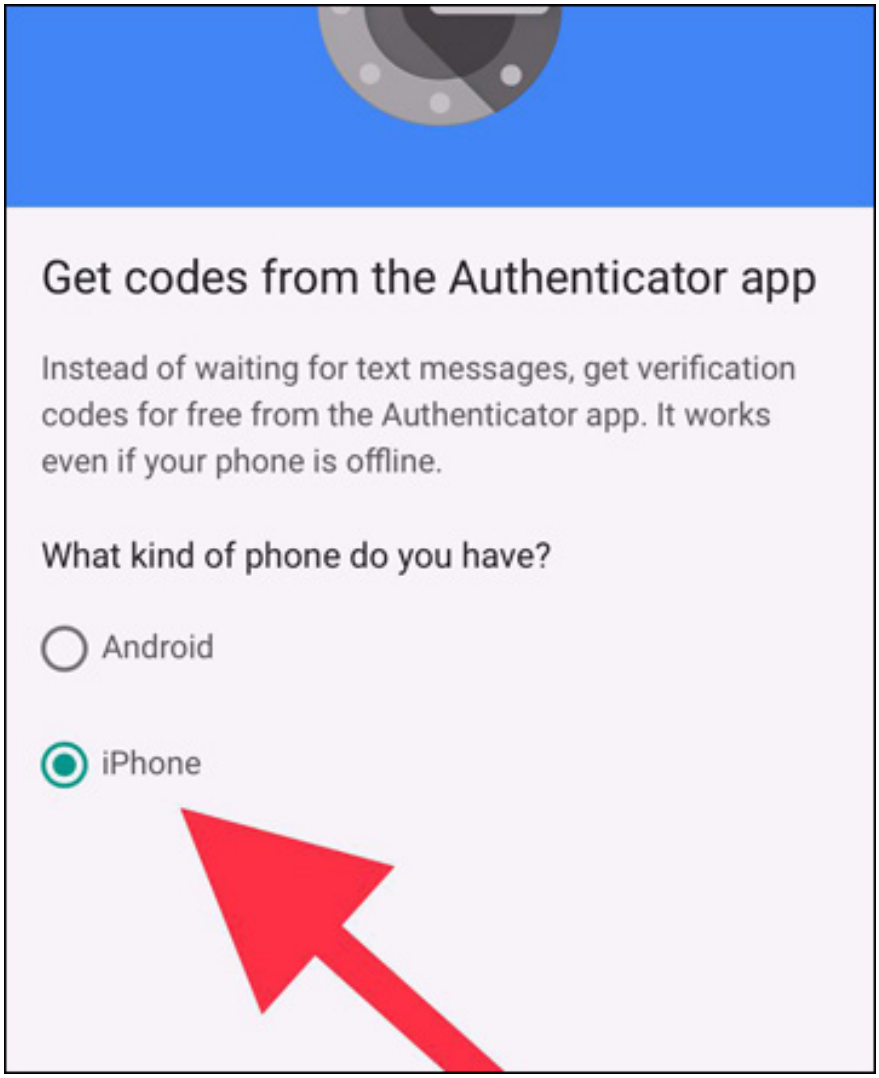
How to set up Google Authenticator

Downloading Google Authenticator app from the App Store store on iOS or Google Play Store on Android is completely free.

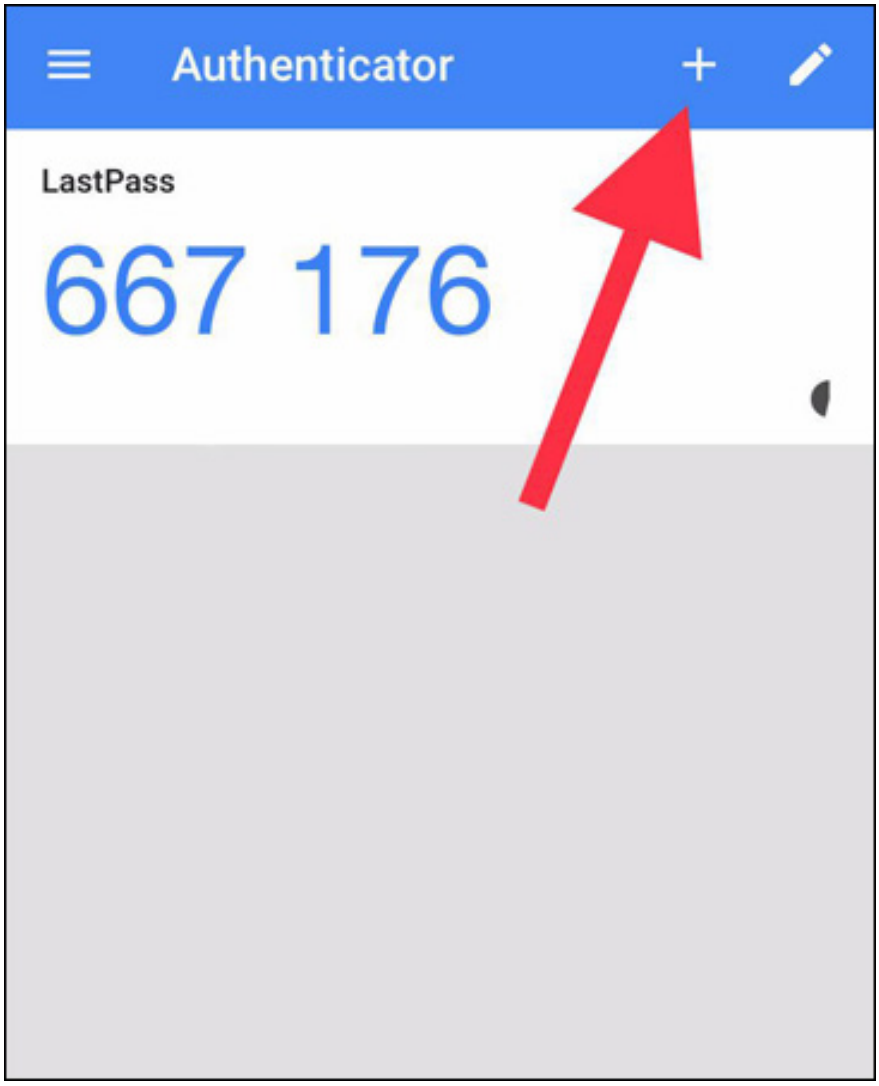
Next, set up 2-step verification on your Google account. Log in to your Google account. In the Security and Sign-In section, select **Two-Step Verification** and scroll down to select the **Authenticator app** .



Select the device you are using: Android or iPhone.

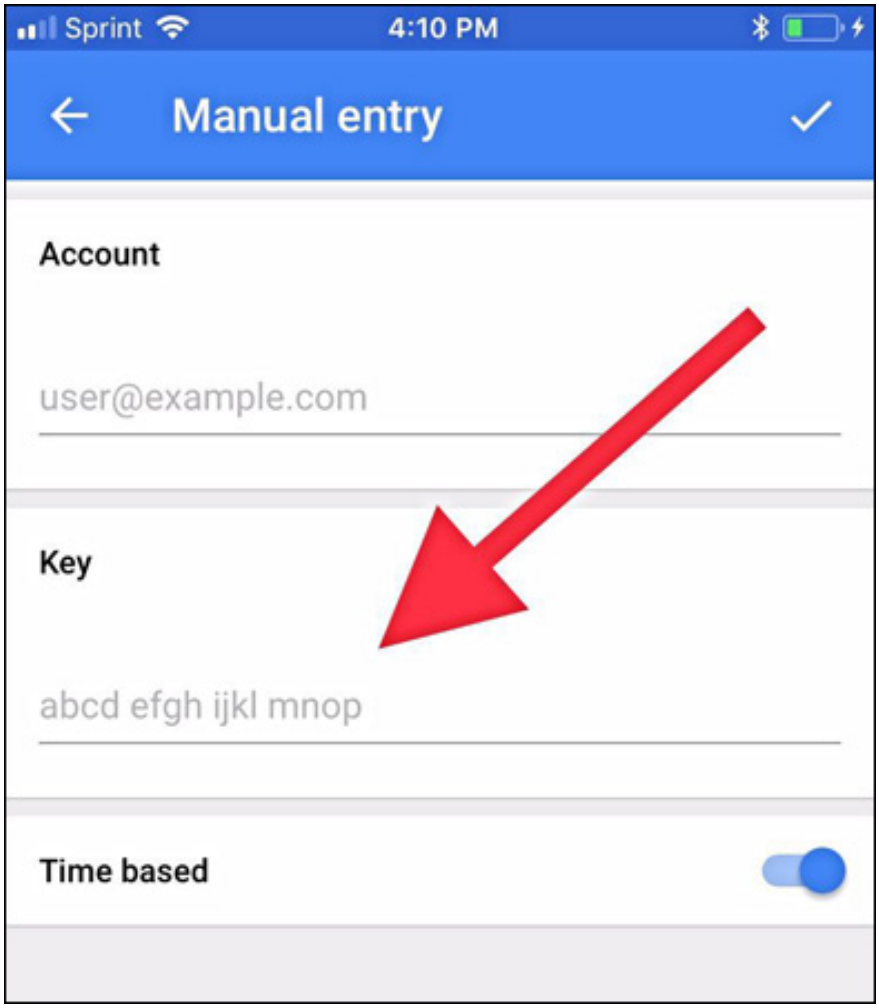


Open the Google Authenticator app on your phone and click the plus sign on the top right of the screen.



At the bottom of the screen, two options are **Scan barcode** and **Manual entry** . You just need to select 1 of these 2 options to complete the process. Scan barcode option will take a long time to complete and other complex so it is better to use Manual entry.

For Manual entry option: Google will send a 16-digit code to your email address. Then you just need to enter that code to complete the verification process.



Make sure you have enabled the **Time Based** option to make sure the code you are entering matches the latest Authenticator code.

Now every time you log in to an account connected to Google Authenticator, the account will ask you to enter a 6-digit verification code. You just need to open the Google Authenticator application, then the application will generate a new random code for you to enter.

Note: If you are always logged in, you will not need to go through the 2FA process anymore.

By using Google Authenticator, your account is not only protected by 2-factor authentication, but also the security layer of Google's 6-digit authentication code.

You finished reading the article "**Google Authenticator adds 'formidable' security layer to email accounts**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.