LIVERPOOL HOPE UNIVERSITY

Liverpool Hope Google account
2-Step Verification (2SV)
Set up Guide

Introduction

2-Step Verification (also known as Multi-Factor Authentication) is an extra layer of security for your Liverpool Hope Google account.

2-Step Verification helps keep out anyone who shouldn't have access to your account by requiring you to verify access to a trusted device after you enter your password. Because 2-Step Verification requires both something you **know** and something you **have**, it's much harder for hackers to gain access. This way, even if your password is stolen, a hacker won't be able to sign in to your account without the physical device.

Authenticator Apps

You will need to download and install an authenticator app (e.g., Microsoft Authenticator, Google Authenticator, Authy etc.) on your smartphone. These apps generate unique, time-sensitive codes that are far more secure than Email, SMS or voice-based methods, which can be vulnerable to interception and SIM-swapping attacks.

Notes:

- This guide will focus on the Microsoft Authenticator app but you can use a different Authenticator app during the Google 2SV set up process.
- Microsoft Authenticator is not available for PC or Mac as authenticator apps are typically designed for smartphones for security reasons.

To install Microsoft Authenticator on your Apple device

- Download and install Authenticator from the Apple app store or scan the QR code below on your smartphone.

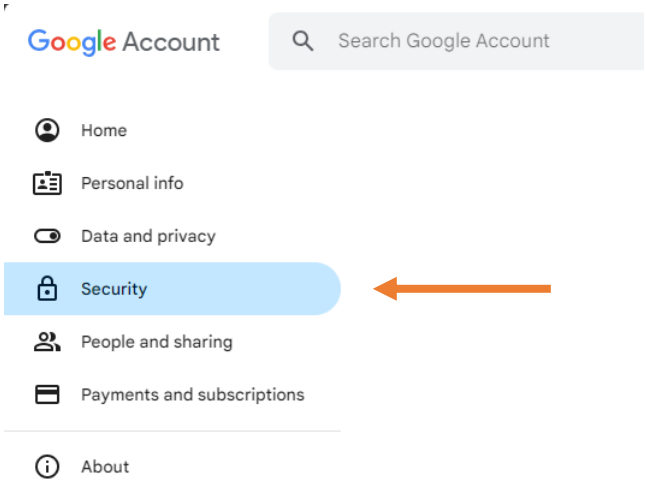
To install Microsoft Authenticator on your Android device

- Download and install Authenticator from the Google Play store or scan the QR code below on your smartphone.

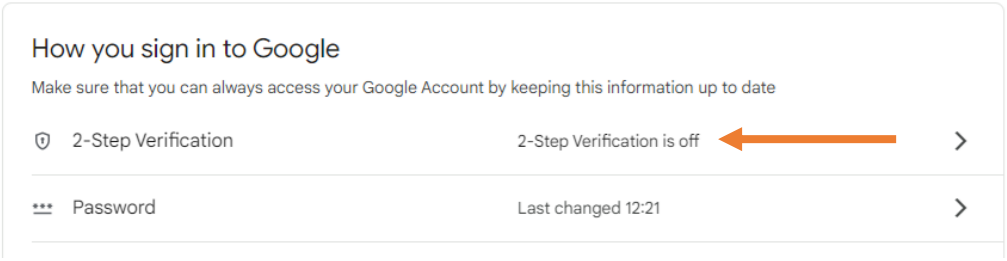
Set up the authenticator app and turn on 2SV

1. On your computer, open a web browser and sign in to your Liverpool Hope Google account.

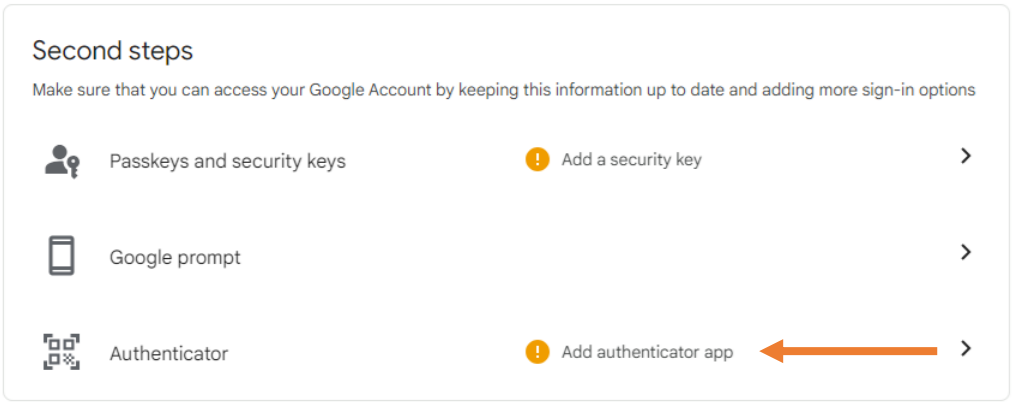
2. In the navigation panel, select **Security**.



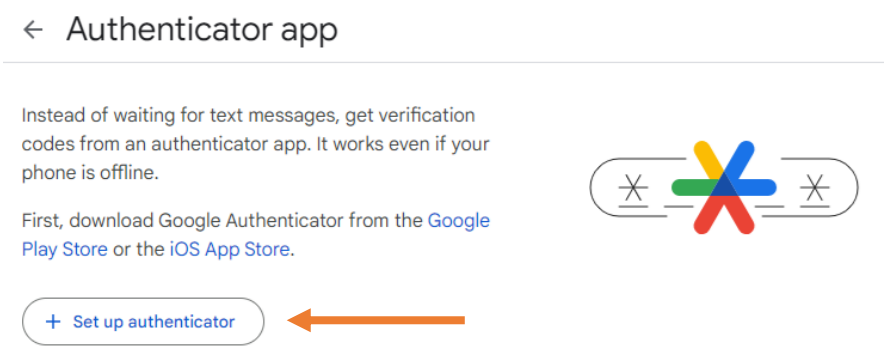
3. On the Google account security page, go to the **How you sign in to Google** section and select **2-Step Verification**.



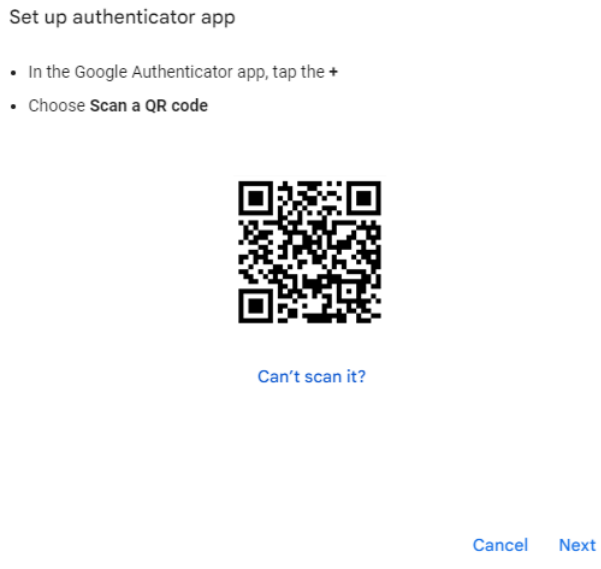
4. On the 2-Step Verification page, select **Add authenticator app** under Second Steps.



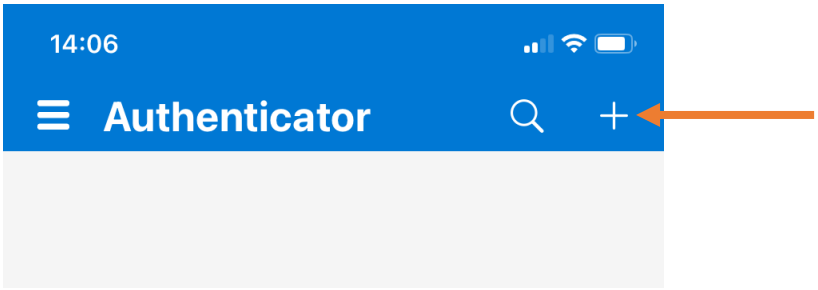
5. On the Authenticator app page, select **Set up authenticator**.



6. You're given a QR code that you can use to automatically associate your account with the Microsoft Authenticator app. **Do not close this window**.

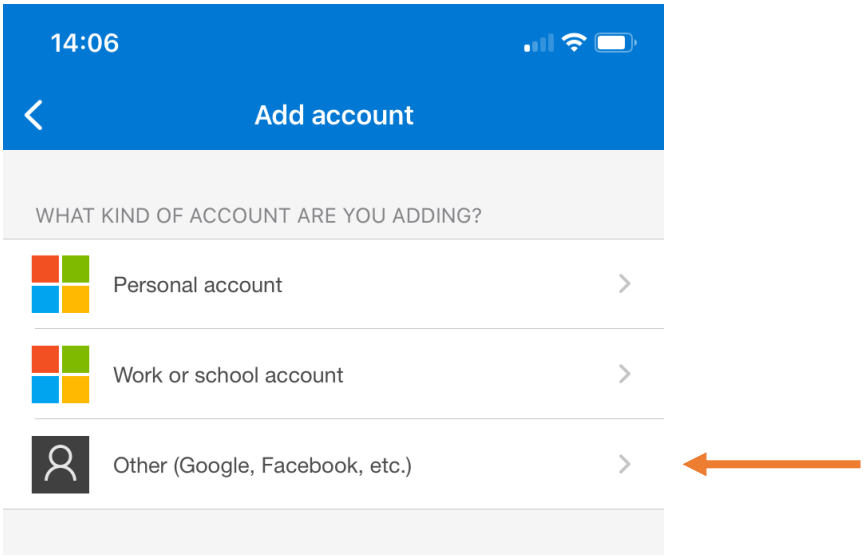


7. Open the Microsoft Authenticator app on your smartphone, select the **Plus** symbol in the upper right.

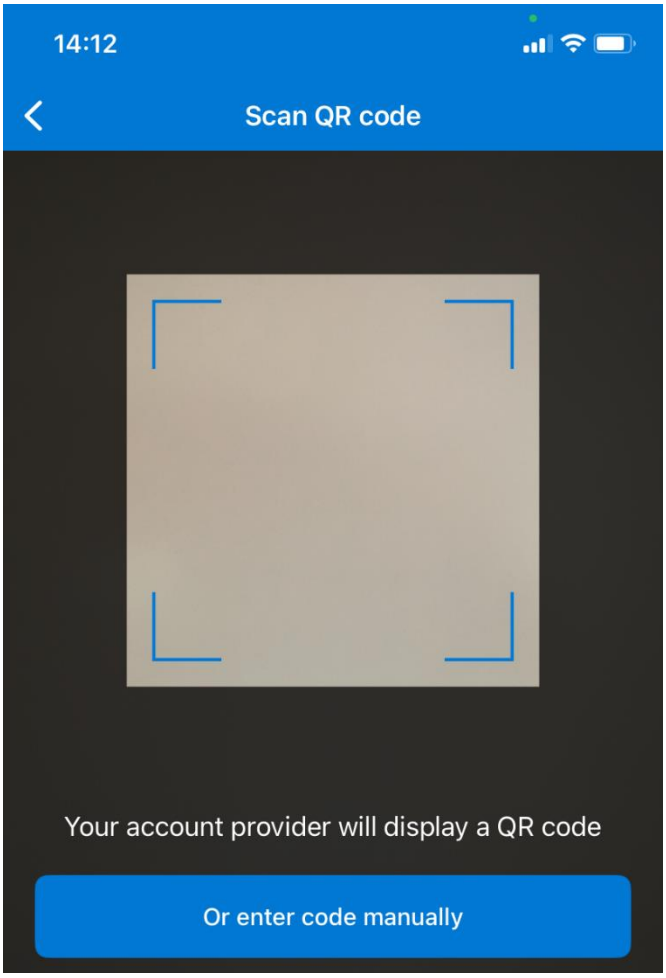


Note: If this is the first time you're setting up Microsoft Authenticator, you might receive a prompt asking you to allow the app to send notifications, access your camera (Apple) or take pictures and record video (Android). Please allow Authenticator to send you notifications for Multi-Factor Authentication and access the camera for scanning QR codes.

8. On the **Add account** screen, select **Other (Google, Facebook, etc.)**.

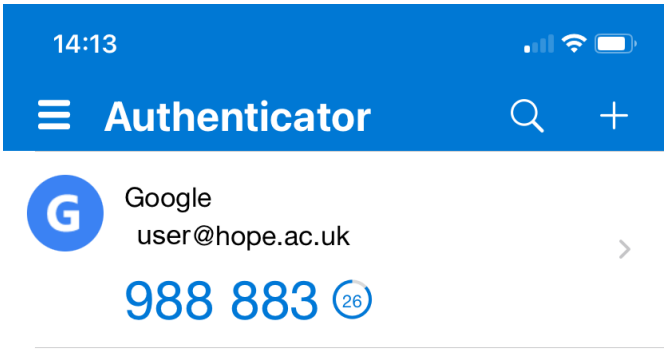


9. Use your smartphone's camera to scan the QR code from the **Set up Authenticator** page on your computer.

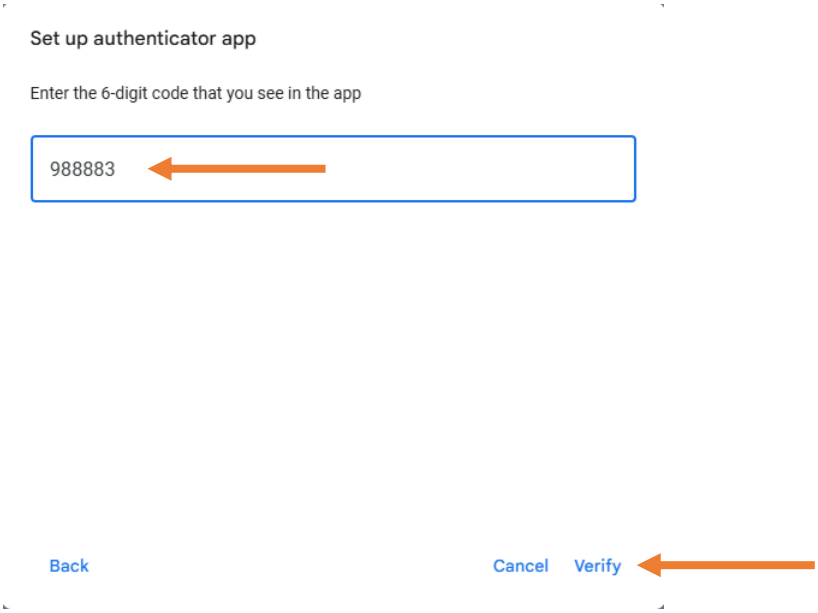


Note: If your camera isn't working properly, you can enter the QR code and URL manually.

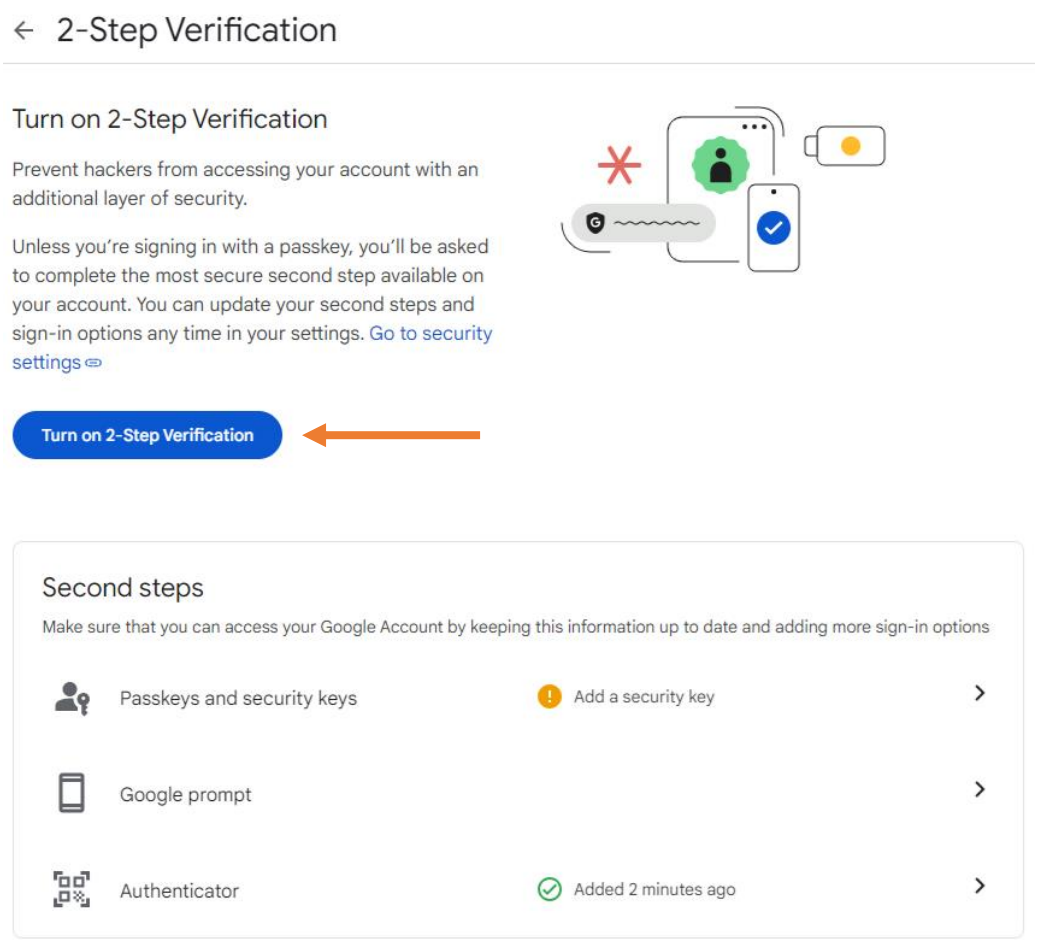
10. Review the Microsoft Authenticator app **Accounts** page on your smartphone, to make sure your account information is right and that there's an associated verification code. For additional security, the verification code changes every 30 seconds preventing someone from using a code multiple times.



11. On your computer, select **Next** on the **Set up Authenticator** page, enter the verification code provided in the app for your Google account, and then select **Verify**.



12. The authenticator app is added to your Google account and you can now select **Turn on 2-Step Verification**.



13. You're now protected with 2-Step Verification and you can select **Done**.