Setting Up Multi-Factor Authentication

What are my options for the second factor ?

All staff will continue to use their current password for their first factor. The following three options are available for the second factor. All three options require your phone to work to varying degrees of privacy. They are listed here in order from "*least private & most convenient"* to "*most private & least convenient"*. The first two methods require you to have an active cell phone or Wifi connection. The last method does not.

1. **Gmail App** (Google Prompt)- For those of you that already have the gmail app installed and regularly check your work email on your phone, this is the easiest, most convenient method. However, having your work gmail on your phone is a personal choice and is the least "private". This is a "*push*" notification and will require connectivity via cell service *or* connecting to wifi (fps-wifi, fpa or PWD).

2. **Text Message pin code** - This method requires that you expose your personal cell phone number to Gmail. While this isn't necessarily a security risk, it is understandable that a person may want to keep their phone number as private and personal as possible. Again, this method will require connectivity via cell service *or* connecting to wifi (fps-wifi, fpa or PWD).

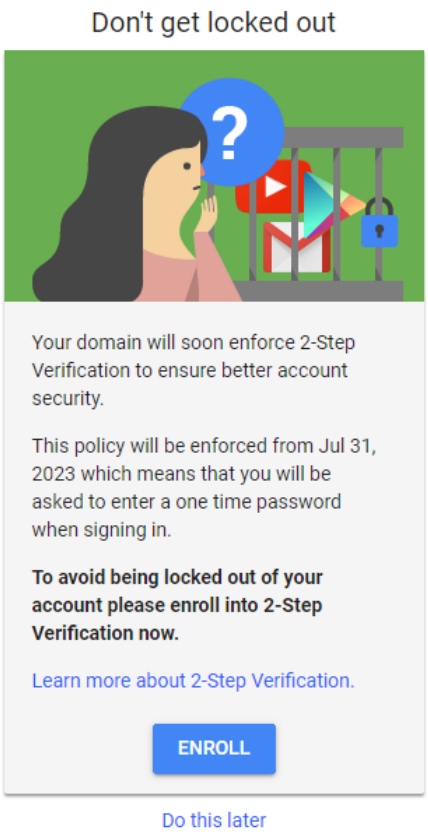
3. **Google Authenticator App** - This method requires you to download an authenticator app and is 100% private. THIS video explains how it works and should help mitigate privacy concerns you may have.

4. Lastly, there is a fourth option for those who do not wish to utilize their cell phone at all. They are called "Backup Codes" These are the least convenient and the least secure as they involve paper-based codes that, in the wrong hands, could be utilized to bypass your MFA login. These codes must also be periodically refreshed and reprinted. Due to their extreme inconvenience, this method is not recommended.

Setting up MFA

After logging in to your google account you will see the message below. (Fig 1) *(note: the date may be different than the one shown below)* . When you are ready, click the “ENROLL” button to begin the process.

Fig 1

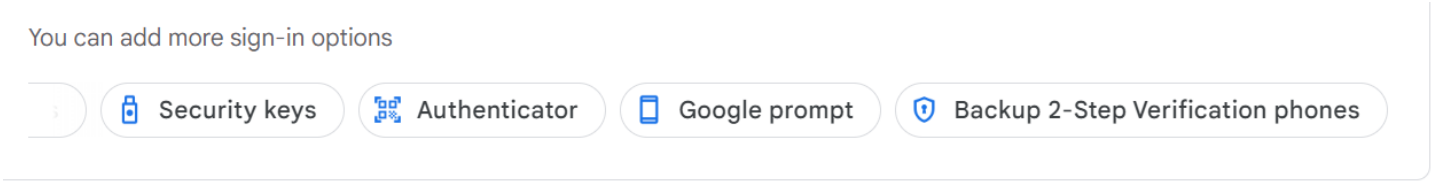


Note that you will be prompted to enter a phone number. If you are planning to use method 3, the Authenticator app, you can use a land-line voice call to receive this code thereby keeping your personal cell phone number private. If you are using methods 1 or 2, you can use your cell phone. Once you enter the code and click “next” , click “TURN ON”.

On the next screen, scroll down a bit and look for the heading “**How you sign into Google**”. There you will see that 2 Step verification has been turned on. At this point, if you used your cell phone in the previous step and prefer to use the text message method for your second factor **(method 2 above)**, you are done ! If, however, you used a landline, you will need to continue in order to add another sign in option for your “second factor”.

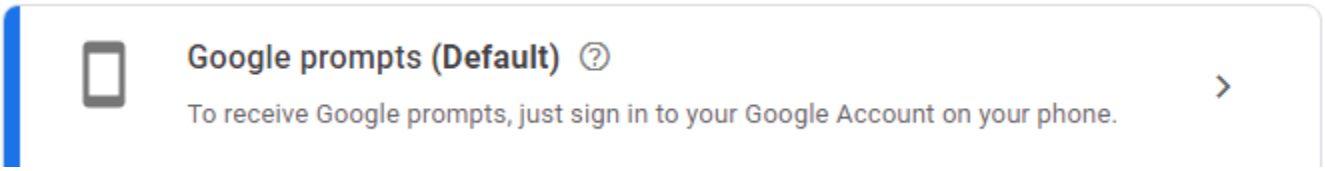
At the bottom of the section look for the options displayed in Fig 2 below. Recommended options are, **Authenticator App** and **Google prompt**. You also may choose Backup 2-Step Verification codes, however these are not recommended due to their inconvenience. If you want to print them to use as an emergency login method, keep them in a safe place (not your desk drawer).

Fig 2



Option 1 - Google GMAIL App
(Google Prompt)

If you already access your work email on your phone, you are 85% of the way to implementing MFA.



When you click this option, Google will display a list of devices you are already logged in to. Possible devices are iPhone, Android or iPad devices. Verify the device(s) shown make sense and that's it ! You're DONE ! If no devices are listed, that means you have not logged into the gmail app on any other device.

Once setup, after you login with your password (factor 1) and you need to authenticate with your second factor, Google will simply ask that you open your Gmail app. It will ask you "Is this you ?" and you just tap "Yes"

Simple and convenient ! However, as stated earlier, you are receiving work email on your personal device, so not necessarily the most private.

Option 3 - Google Authenticator App
NOTE: *This option is recommended as it is the most convenient and does not require cell or wifi connection to work making it suitable for use in buildings with limited service.*

1. Install Google Authenticator App on your phone (iPhone or Android) by clicking this link (while using your phone) or by searching for it in the App Store associated with your device. Once installed, open the app. You should see "add new" and a selection to scan a QR Code. Put your phone aside for now.

2. Follow steps shown on your computer screen to display the QR code. Next, to scan the QR code using the Authenticator App on your phone. Click the "+" in the bottom right corner of the App to add / scan the QR code. You may need to give the App access to your camera in order to make this work.

3. Once setup, when you open the app you will see a 6 digit code that changes about every 30 seconds. These codes will work and be available regardless of your connectivity to the internet so they are a good option for areas of limited connectivity.

4. Finally, as a reminder, this app does not expose your personal information or identity to anyone. It simply provides a code to use as your second factor. Click here to see why it is completely private.