Document Name

Securing Online Accounts

Two-Factors Authentication

WHAT IS TWO-FACTOR AUTHENTICATION?

Two-factor authentication (2FA) is a process that typically requires a combination of something a user knows (pin, secret question) and something a user has (cards, fingerprint) in order to access a program or operating system.

WHY IS IT IMPORTANT TO TURN 2FA ON?

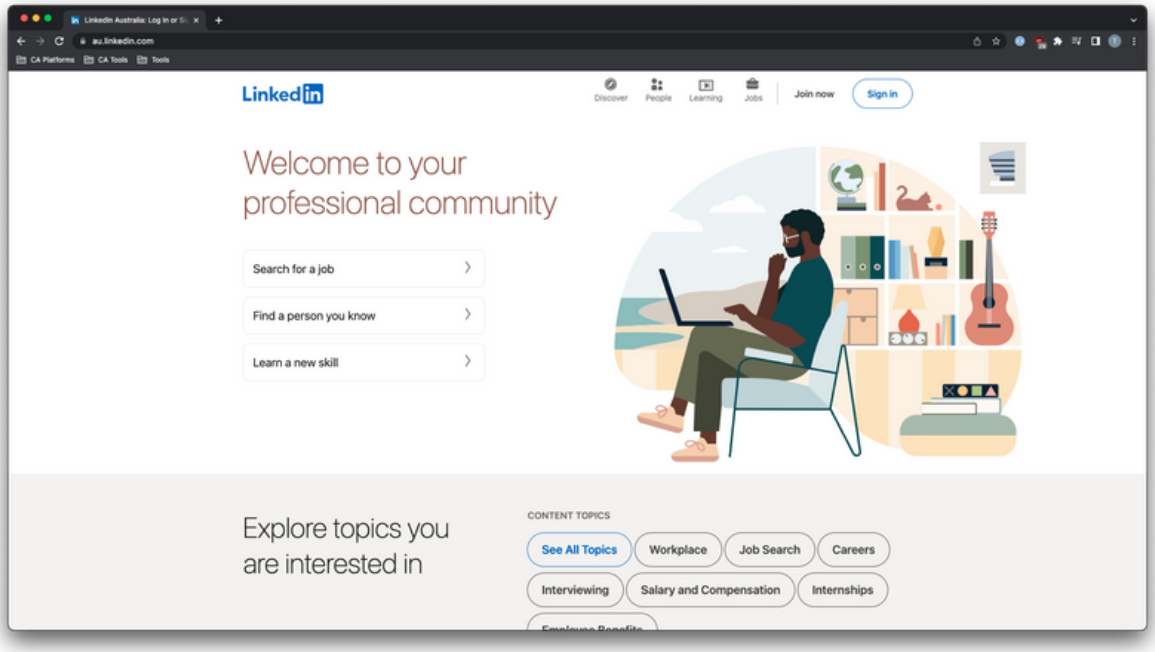
Using 2FA to access your favourite programs provides enhanced security to traditional usernames and passwords. The multiple layers of authentication increase confidence that the user requesting access is who they claim to
be i.e., you.

WHERE DO I TURN IT ON?

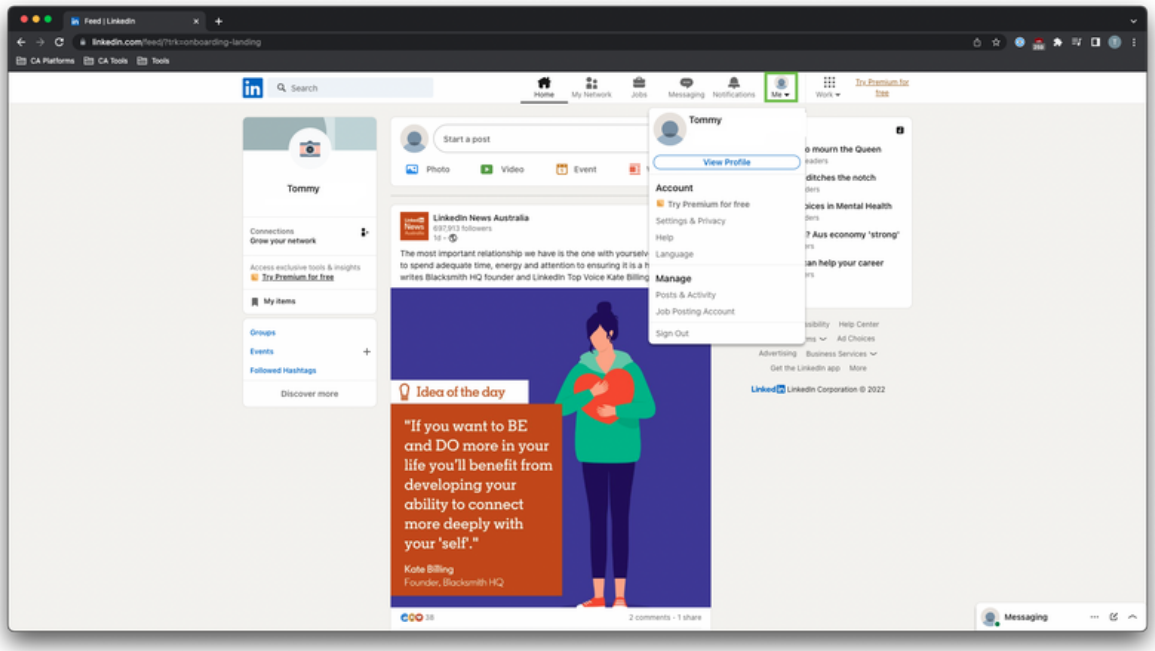
Where to turn on 2FA within a program depends on each program. However, the steps are universally simple and somewhat similar. Icons and language may differ slightly depending on the program, or device you are using.

Setting up 2FA for LinkedIn browser

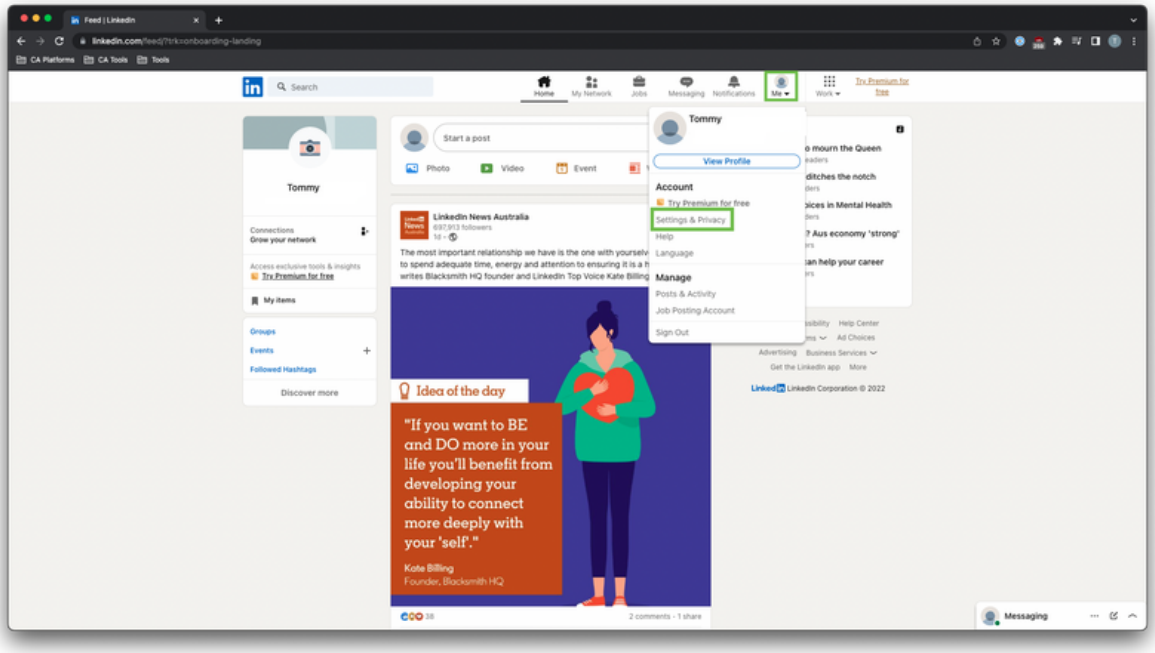
1. Open LinkedIn



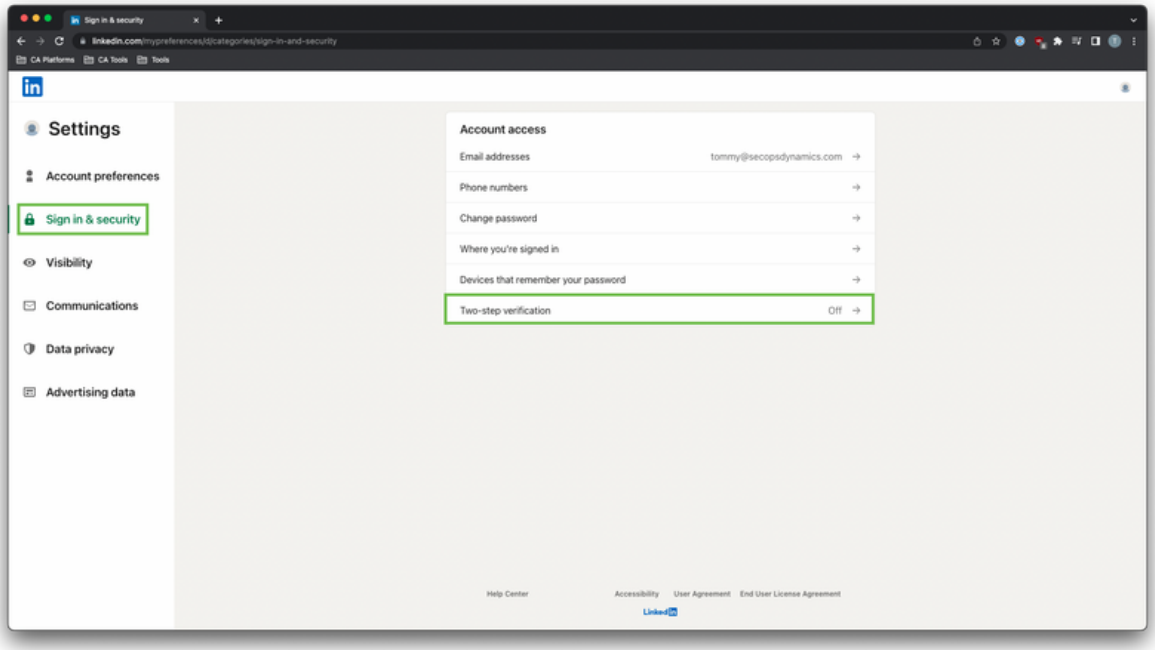
2. Click the Me icon at the top of your homepage



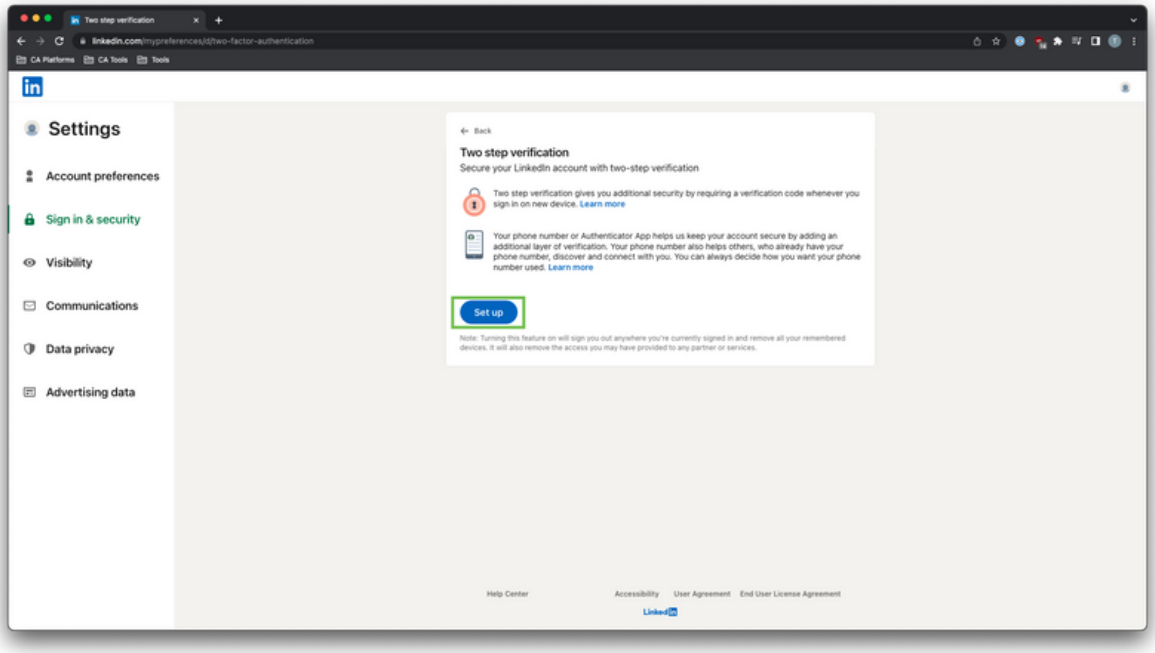
3. Select Settings & Privacy from the dropdown



4. Under the Sign In and security section of the Account tab, click the arrow icon next to Two-step verification

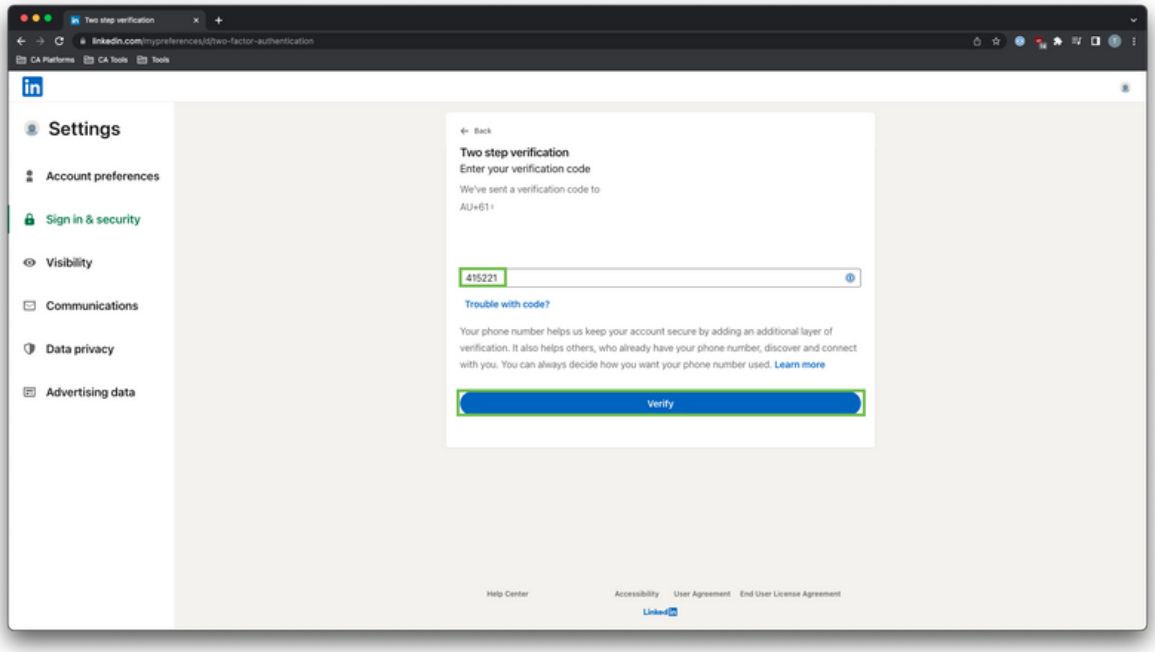


5. Click Setup



Note: You may be asked to enter your password or verificationcode (if your mobile number is linked to your account) for security reasons

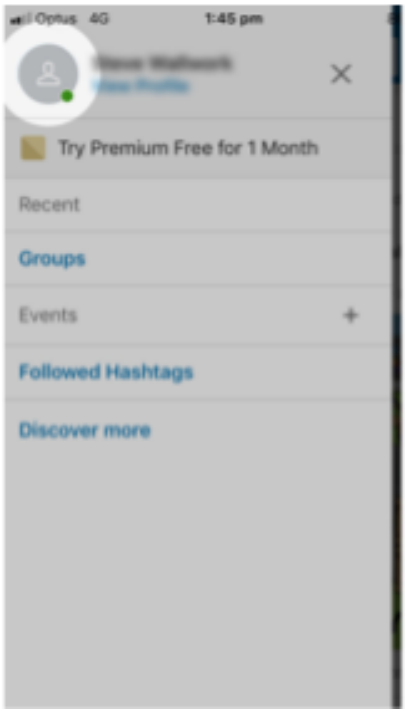
6. Once you receive a code sent to your phone, enter it into the box on the device you're using to sign in and click Verify



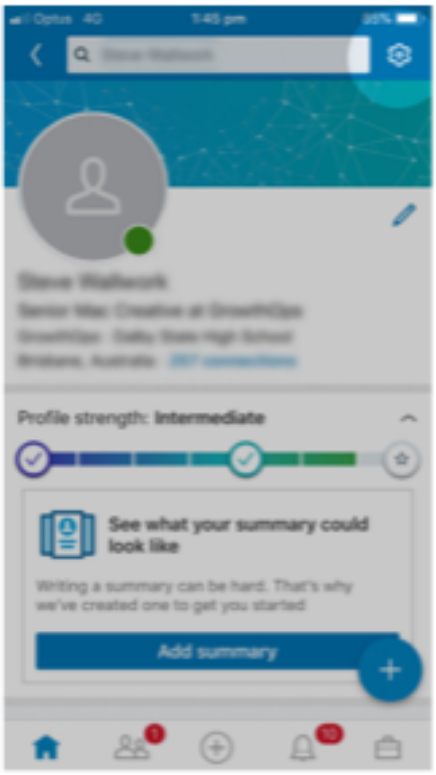
Setting up 2FA for LinkedIn Mobile App

1. Open the LinkedIn app

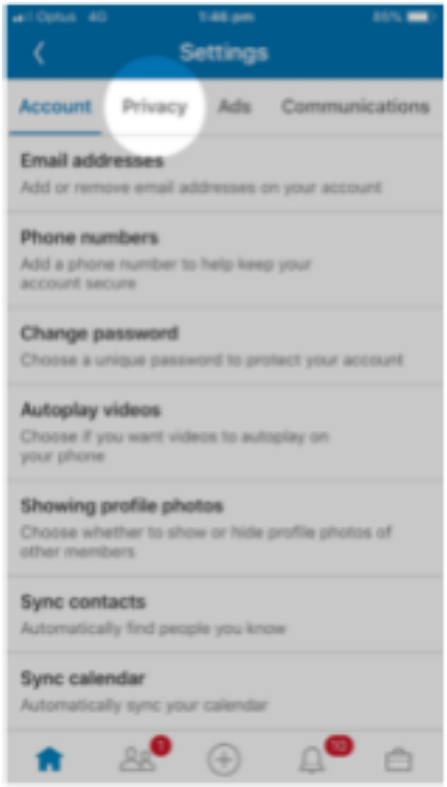
2. Tap your Profile picture



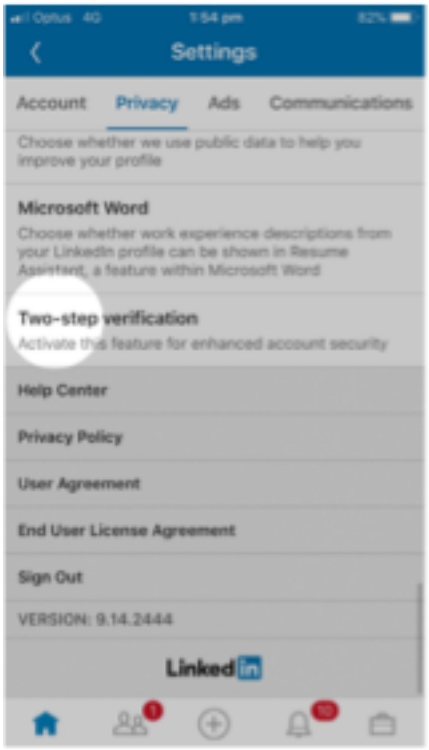
3. Tap the Settings Icon in the top right



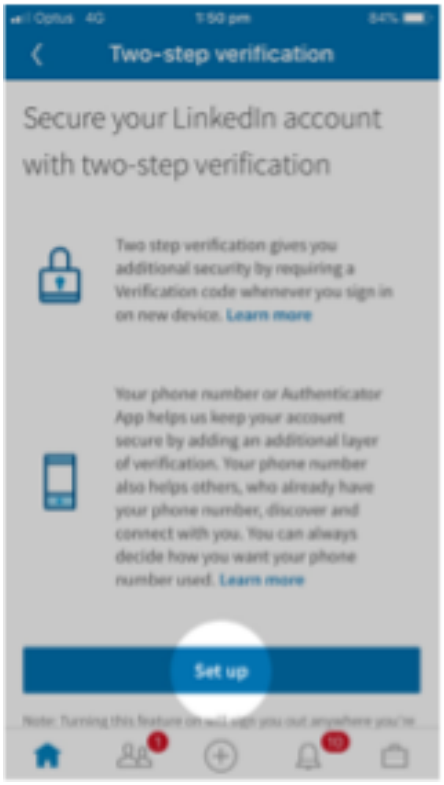
4. Tap the Privacy tab



5. Scroll to bottom of screen and tap Two-step verification



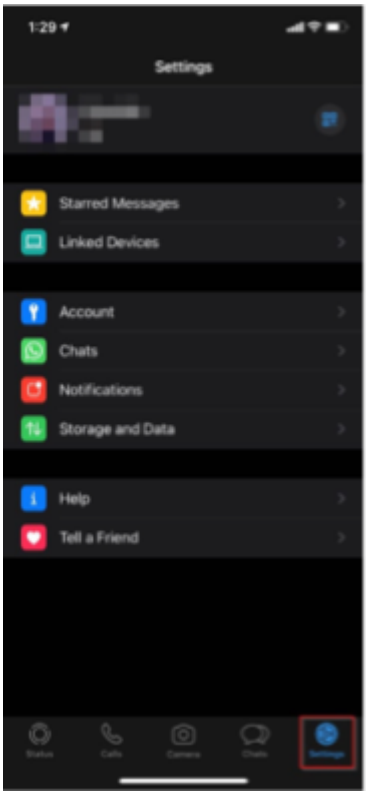
6. Click on Setup then follow the instructions on-screen



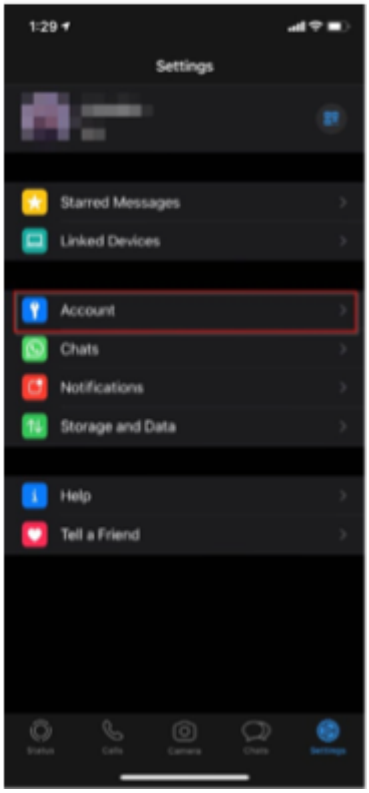
Setting up 2FA for WhatsApp Mobile App

MFA for WhatsApp is called two-step verification. Two-step verification requires you to enter a six digit Pin before gaining access to your account. Once MFA is set up, WhatsApp will periodically ask you to enter your Pin.

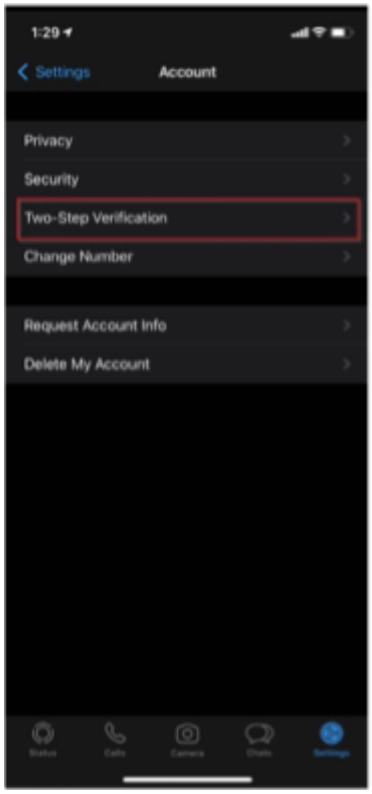
1. In WhatsApp or WhatsApp Business, select the Settings icon in the bottom right-hand corner.
If you use an Android device, you may have to access Settings by tapping three vertical dots in the upper right-hand corner of your screen.



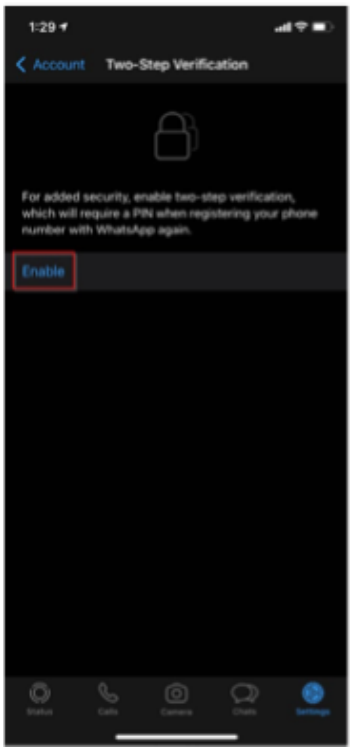
2. Select Account.



3. Select Two-Step Verification.

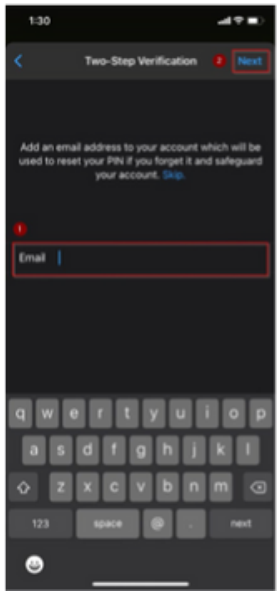


4. Select Enable.

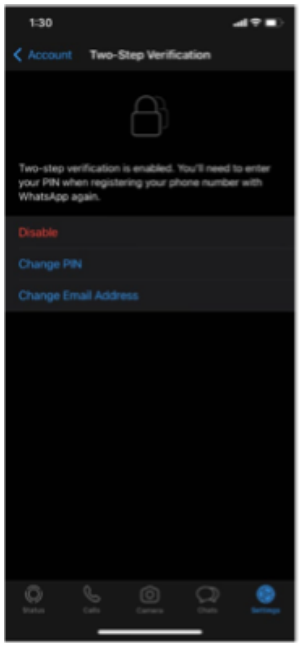


5. Enter a six-digit Pin, You will then be asked to confirm your Pin. When complete, select Next.

6. Enter your Email address and select Next. Then confirm your email address and select Done. This step is optional but will allow you to reset your Pin if you forget it.



7. After enabling two-step verification, you will be returned to this page. The setup is now complete.
You can return to this page in the future if you need to change your Pin or recovery email address.



WhatsApp Security codes to verify Contacts

Security codes are used to verify the identity of a contact and the security of one-to-one messages and calls.

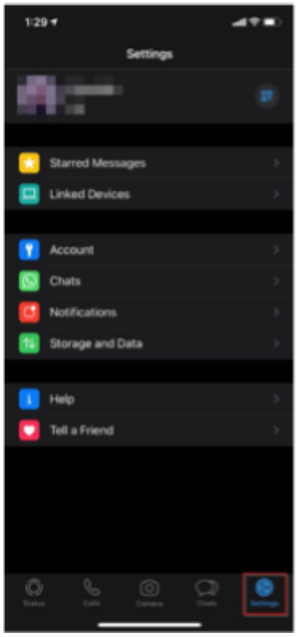
They verify messages and calls are secure and that no one is intercepting or altering your communications. This is done by scanning the QR code on your contact's device or verifying the 60-digit safety number exactly matches on both devices.

Security codes usually, but not always, change when a contact reinstalls the app, changes phone numbers or changes devices. Users should verify with the contact as to why the safety number has changed. Users should also be on the lookout for frequent or unexpected changes as this is a sign something may be wrong.

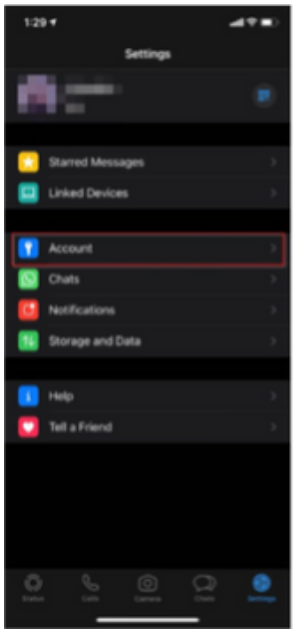
The following guide has been broken up into two sections. The first section shows how to enable notifications for when a security code changes. The second section shows how to verify the security code of your contact to ensure you are messaging the correct person. The contact will remain verified until the security code changes.

HOW TO ENABLE NOTIFICATIONS WHEN A SECURITY CODE CH

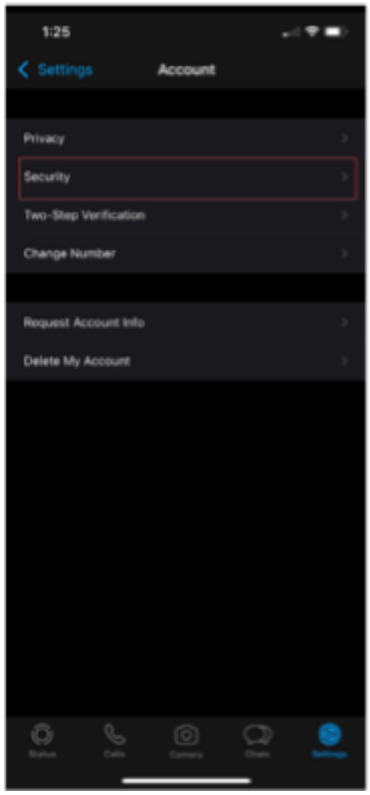
1. In WhatsApp or WhatsApp Business, select the Settings icon in the bottom right-hand corner.
If you use an Android device, you may have to access Settings by tapping three vertical dots in the upper right-hand corner of your screen.



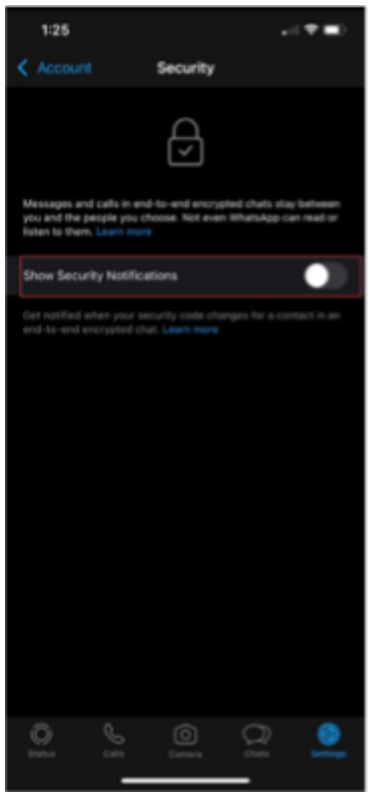
2. Select Account.



3. Select Security.

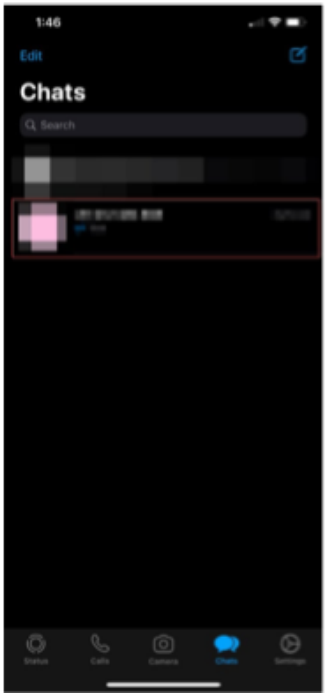


4. Turn on Show Security Notifications.

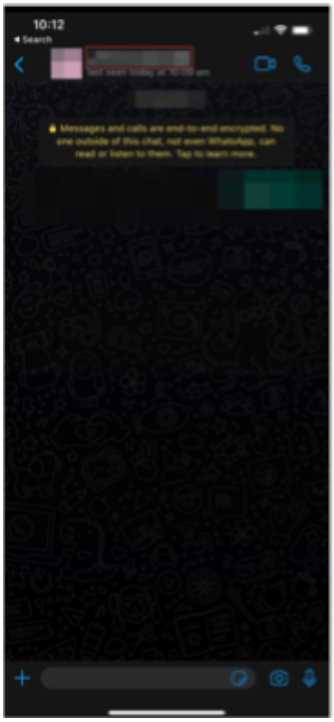


HOW TO VERIFY WHATSAPP SECURITY CODES

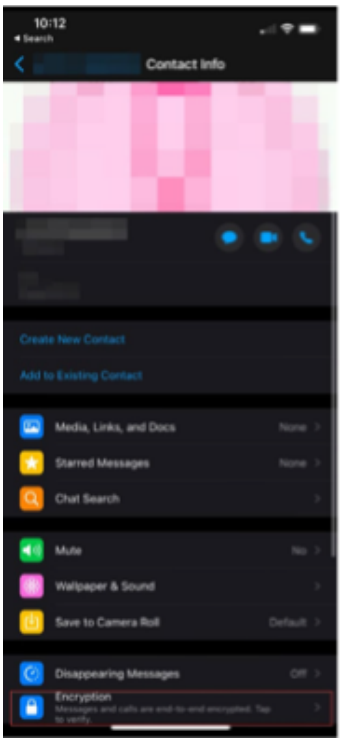
1. To verify the security code of a contact, select Chats and select the one-to-one conversation you wish to verify.



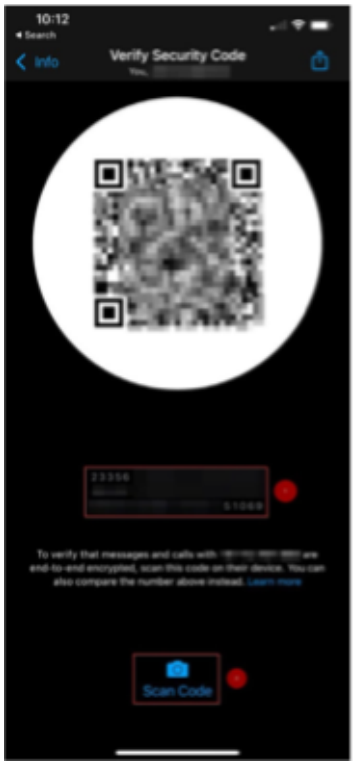
2. Select the name/number of the contact.



3. Select Encryption.



4. To check the security code, either scan the QR code on the other person's device or verify the 60-digit number matches on their device. You can send the number to them using the share button.



Only share the security code using trusted methods of communication, where you have verified that the other person is who they say they are (such as a phone call where you recognise the person's voice).

Be wary of communication methods that could be intercepted or compromised, such as email. Consider splitting parts of the code across multiple communication methods to stay secure and don't use a WhatsApp message to the contact you are verifying as a method of verification.

Once all steps are completed, you will have verified the contact and will be notified if their security code changes.

Turn on MFA for your Microsoft Account

These steps will show you how to turn on MFA for your Microsoft Account.

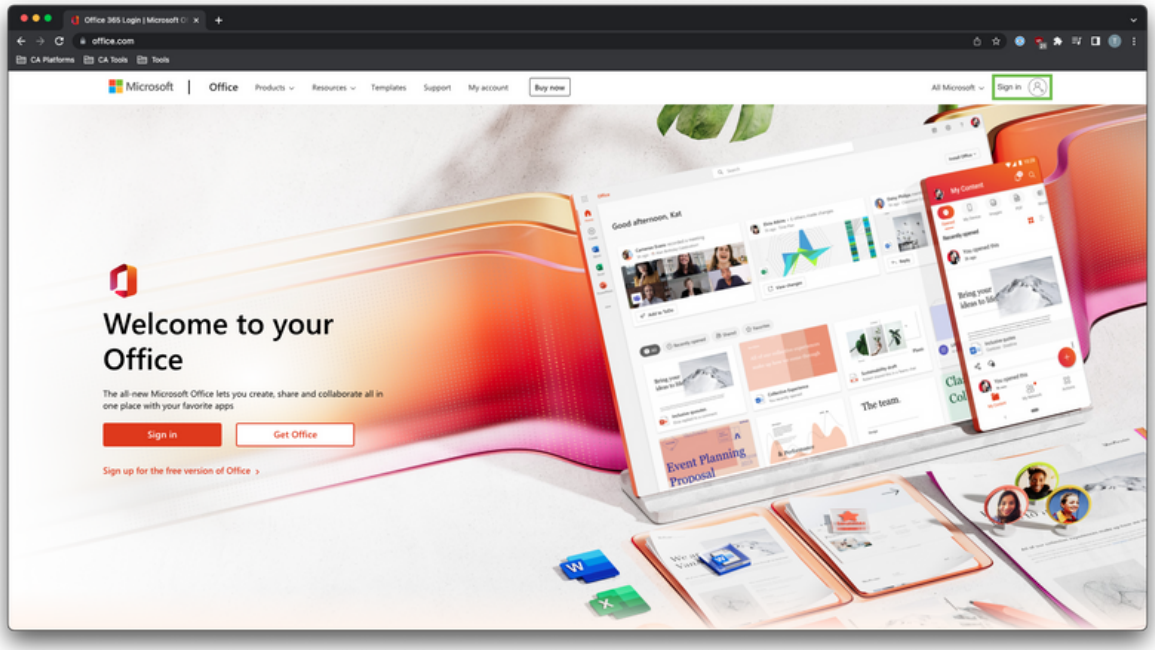
After you turn on MFA, you'll need both your password and an additional authentication method to log in to your Microsoft account. This could be a security code from an authenticator app, SMS, or phone call. Alternatively, you could get a notification to the Microsoft authenticator app on your smartphone.

MFA makes it harder for cybercriminals to access your account and it could also alert you to any suspicious activity. This means if your password is guessed or stolen and a cybercriminal is trying to login to your account, you will be sent a security code or notification. This will prevent them from logging in to your account as they won't have the security code, or you can deny them entry if you use the Microsoft authenticator app. You can then change your password to secure your account.

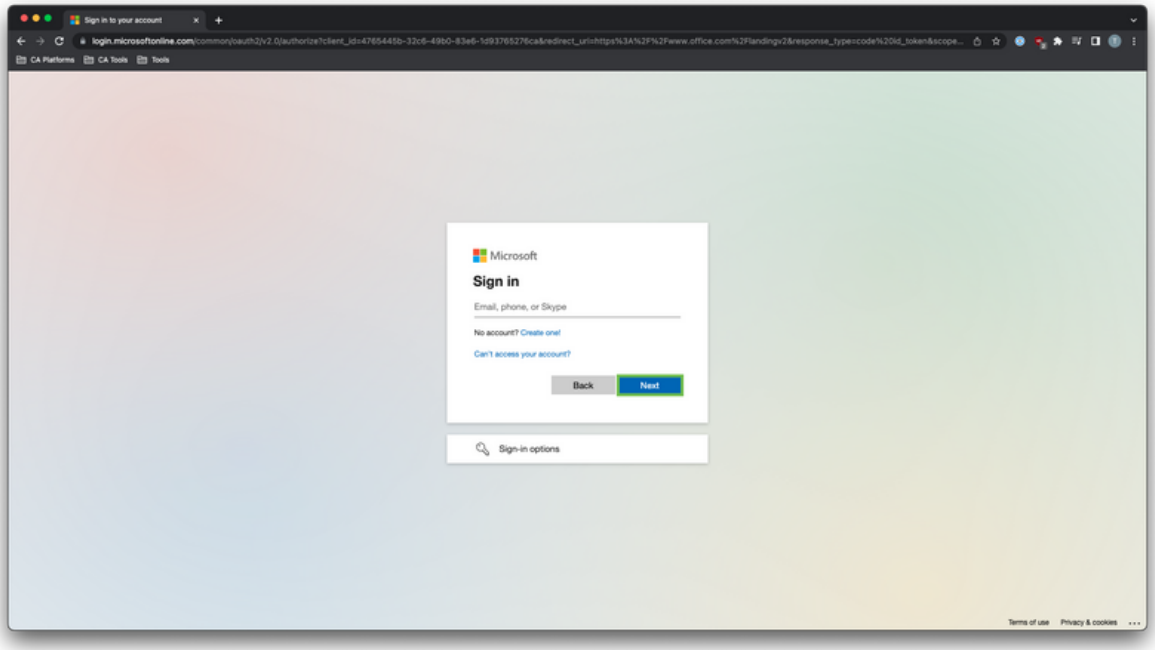
If you don't have MFA turned on, you may not get notifications on attempts to log in to your account.

This guide will show you how to set up MFA for your Microsoft Account on your computer. If you don't have access to a computer, you can follow these steps on any device, however some screens may appear different than pictured.

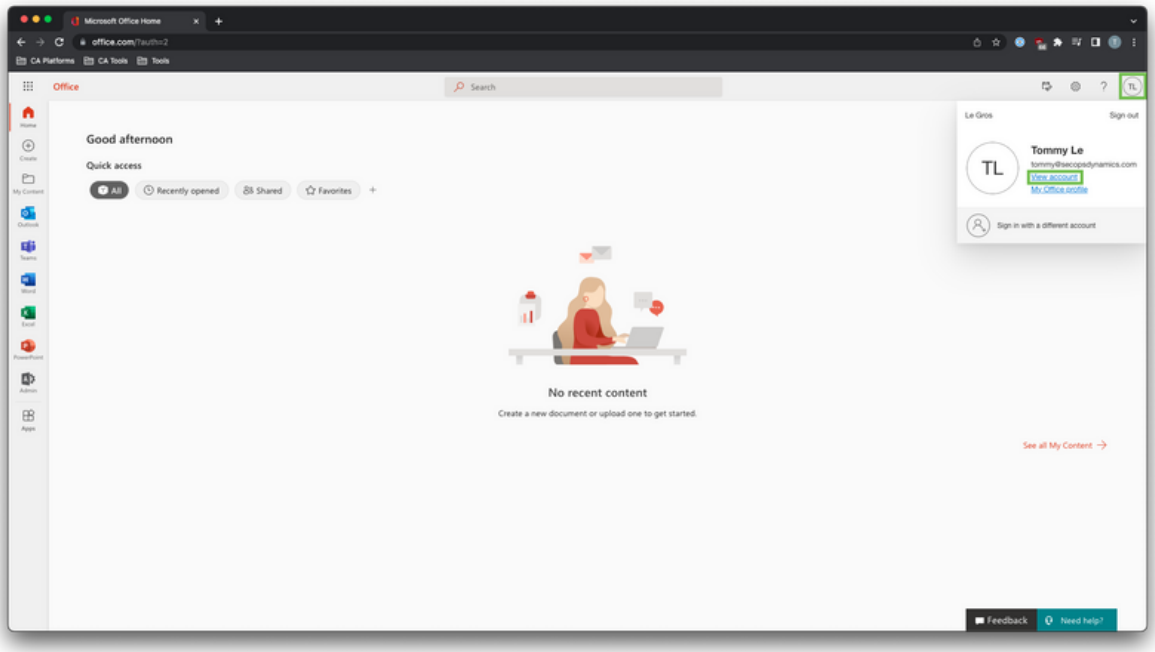
1. Open an internet browser (for example Google Chrome, Microsoft Edge, Mozilla Firefox or Opera). Go to the Microsoft Office website (https://office.com) and select Sign in in the top right corner.



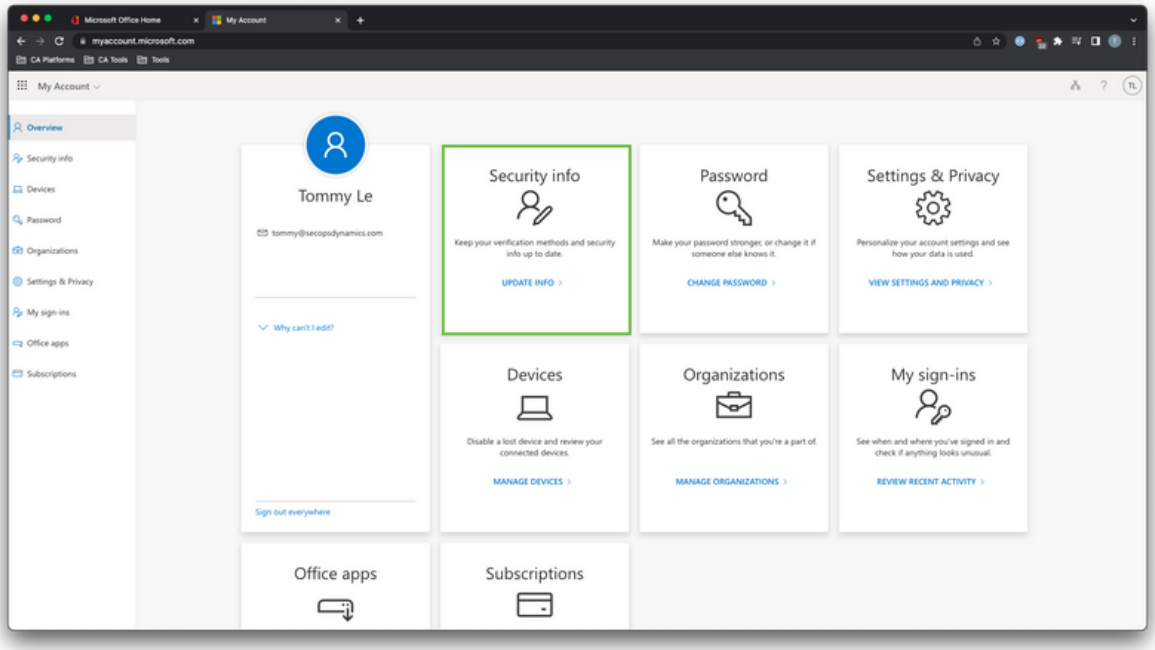
2. Enter your sign in information and select Next and then enter your passphrase and select Sign in.



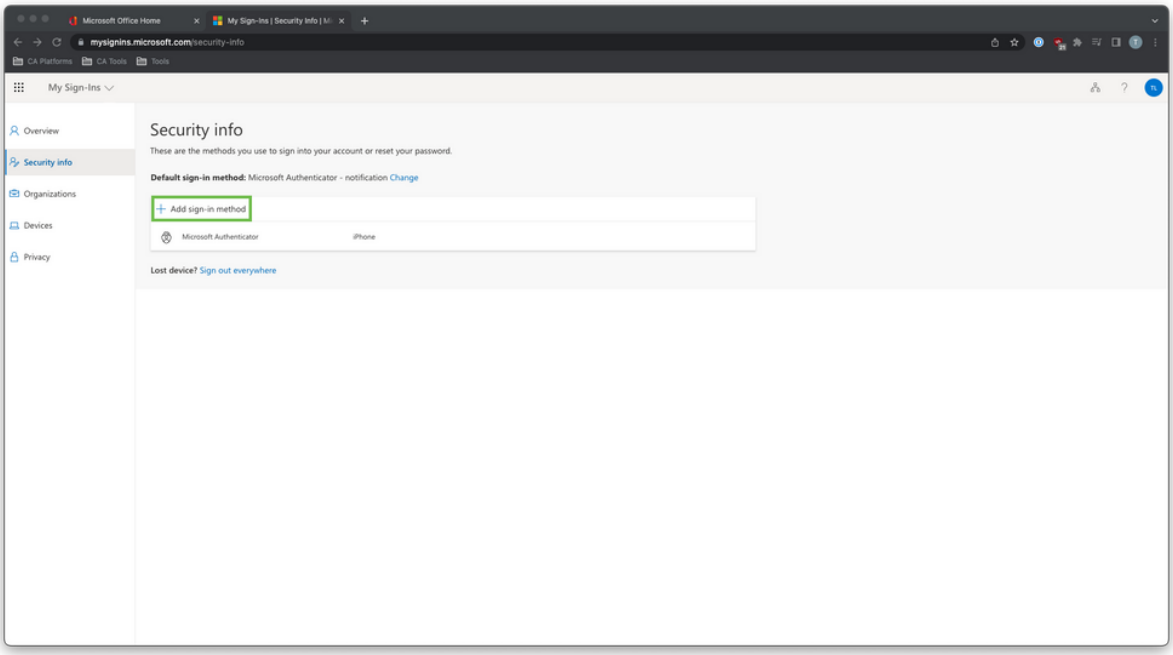
3. Select your account profile icon or picture in the top right of the screen and select View Account.



4. Select Security Info



5. Select Add sign-in method.
If you don't already have a recovery method for your account (such as an alternate email address or phone number) you will now be prompted to set one up.
A recovery method can help you get back into your account if you lose access.
Follow the on-screen prompts to set up a recovery method.

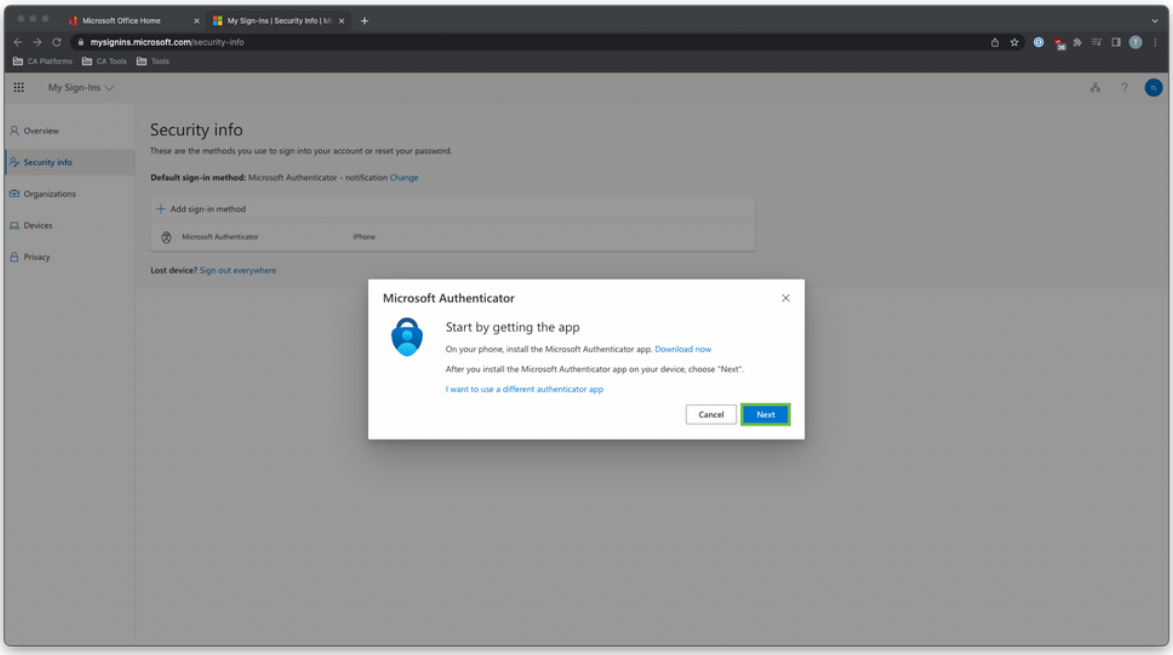


"You may see a prompt abou

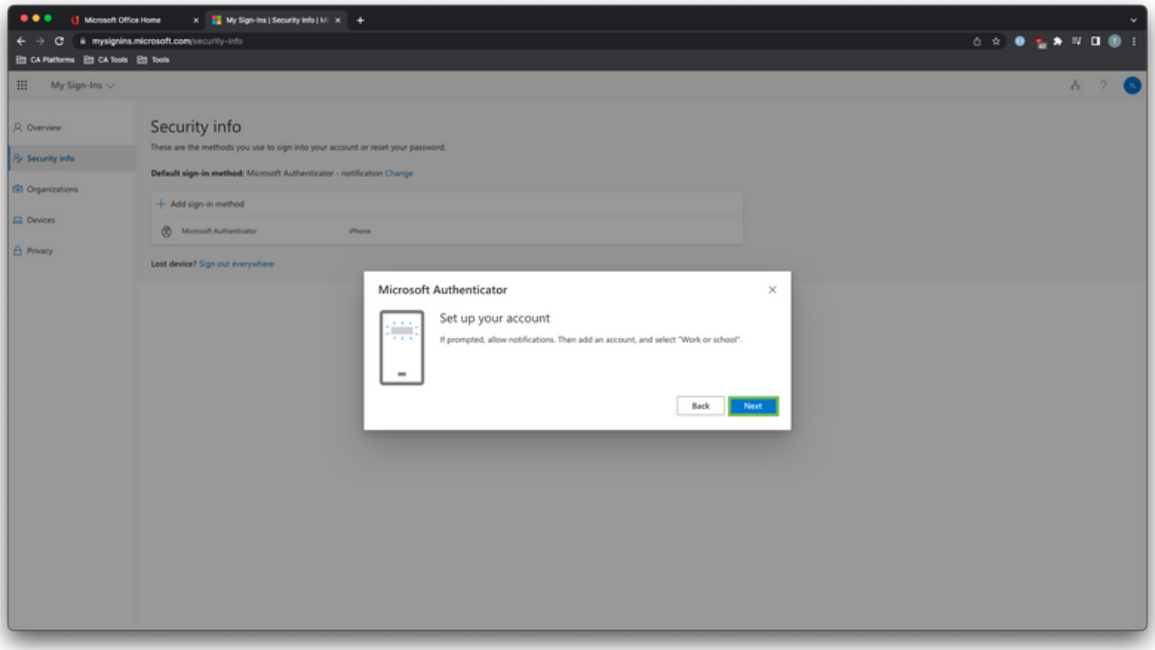
password'. This is a feature offered by Microsoft and an alternative to setting up your account with a password. For more information, see Microsoft's official website.
(https://support.microsoft.com/en-au/account-billing/how-to-go-passwordless- with-your-microsoft-account-674ce301-3574-4387-a93d-916751764c43)

"

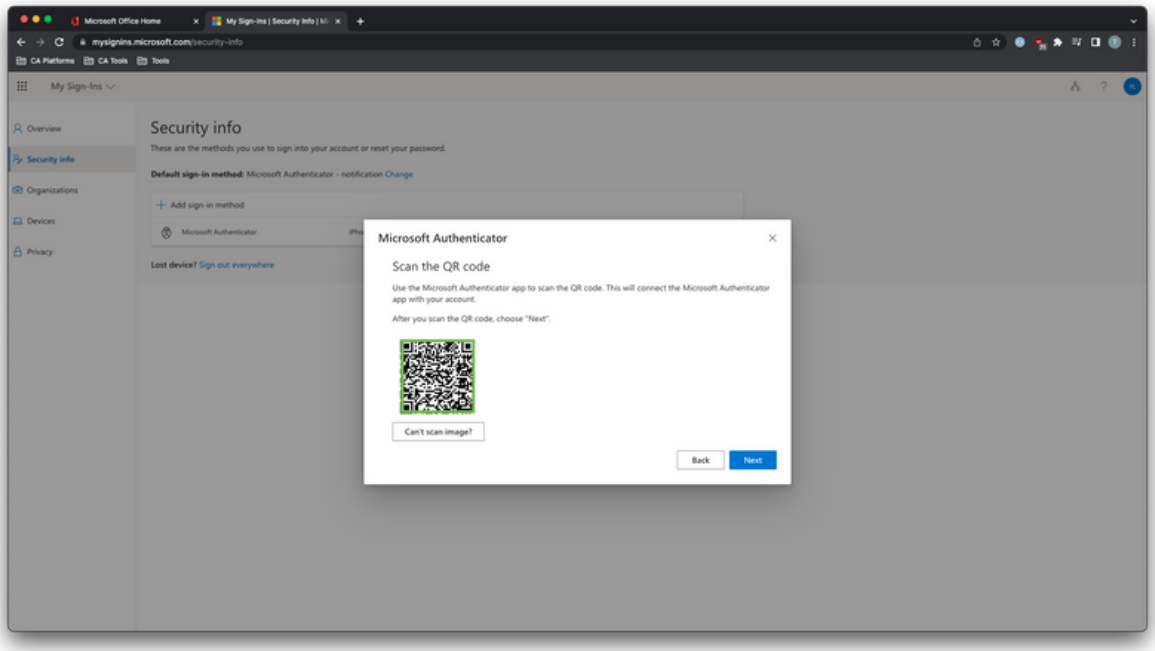
6. Select Authenticator App under ‘Add sign-in method’.



7. Read the information and select Next.



8. Open the authenticator app on your smartphone and scan the QR code. Enter the code generated by the app and select Next.



Store your recovery code in a secure place and create a backup of it in a secondary place. This will help you access your account if you lose access to your authenticator app. Select Next.

9. If you have an app or smartphone that needs an app password, follow the on-screen prompts for your device. Most modern smartphones and apps accept security codes, so an app password won't be necessary. Select Next if you do not require an app password.

10. If you have an older device or application that cannot accept a security code (for example an Xbox 360 or Microsoft Office 2010 or earlier) you can create an app password. Follow the on-screen prompts to learn more about app passwords. If you do not require an app password, select Finish.

"If you replace your smartphone, remember to moveyour authenticator app to the new device by using the backup and recovery feature."

Additional Security Tips

ADD SECURITY INFORMATION

Additional security information is a phone number or alternate email address used to contact you or send you security codes if your account is compromised.

For more information see Microsoft's website (https://support.
microsoft .com/en-us/account-billing/how- to -
add-security-info-to-your-microsoft-account-
9df 3f 37f-3659-cbb1-75ba-6cb41c1bff45).

USE PASSWORDLESS

Passwordless is a way to securely sign into your account without a password. Instead, you sign in with your username and then confirm it is you with the Microsoft Authenticator app on your phone.

For more information see Microsoft's website (https://support.
microsoft .com/en-au/account-billing/how- to -
go-passwordless-with-your-microsoft-account-
674ce301-3574-4387-a93d-916751764c43).

DON'T SHARE MFA CODES OR APPROVE UNKNOWN SIGN IN ATTEMPTS

Requests for sign in approval and the security codes you get are Microsoft's way of checking that you are the person who signed in. If you give
someone else your MFA code or approve unknown sign in attempts, then someone else might be able to log into your account. Never approve unknown sign in attempts or give anyone else your MFA code.

TRANSFER YOUR AUTHENTICATOR WHEN CHANGING DEVICES

If you are using an authenticator app for MFA and you get a new device, make sure you transfer it to your new device before disposing of or resetting the old one. We recommend adding a recovery method to your account and saving your backup codes in case you lose access to your authenticator app.

KEEP YOUR APPS UP TO DATE

For security reasons it is important to keep your apps up to date. Wherever you are logged into your account, make sure the apps are up to date, whether it be an internet browser, Microsoft Office, email or other apps on your phone. Updates often include important security upgrades.

KEEP YOUR OS UP TO DATE

It is also important to keep your operating system up to date. Updates will have important security upgrades. Ensure that all computers and phones have the most recent version of software and if a device is no longer supported by software updates or security updates, consider replacing it.

CHECK YOUR RECENT ACTIVITY

If you receive an email notifying you of unusual activity, you can see when and where your account has been accessed—including successful sign-ins and security challenges— on the Recent activity page. Microsoft learns how you usually sign into your account and flags events that are suspicious.

KEEP YOUR DEVICES SAFE

If you lose or give away a device that you use to sign into your Microsoft account, or if you know that someone else has access to your devices for whatever reason, be proactive and remove the trusted status from your devices.

To remove trusted devices, go to the Security basics page, select more security options, scroll down to Trusted Devices, and then select Remove all the trusted devices associated with my account.

For more information, see how to add a trusted device to your Microsoft account (https://support.microsoft.com/en-us/account-billing/add-a-trusted-device-to-your-microsoft-account-fe3860c8-bc04-9770-e218- b4fd6b767f4b)

Turn on MFA for your Google Account

These steps will show you how to turn on MFA for your Google Account. After you turn on MFA, you'll need both your password and an additional authentication method to log in to your Google account.

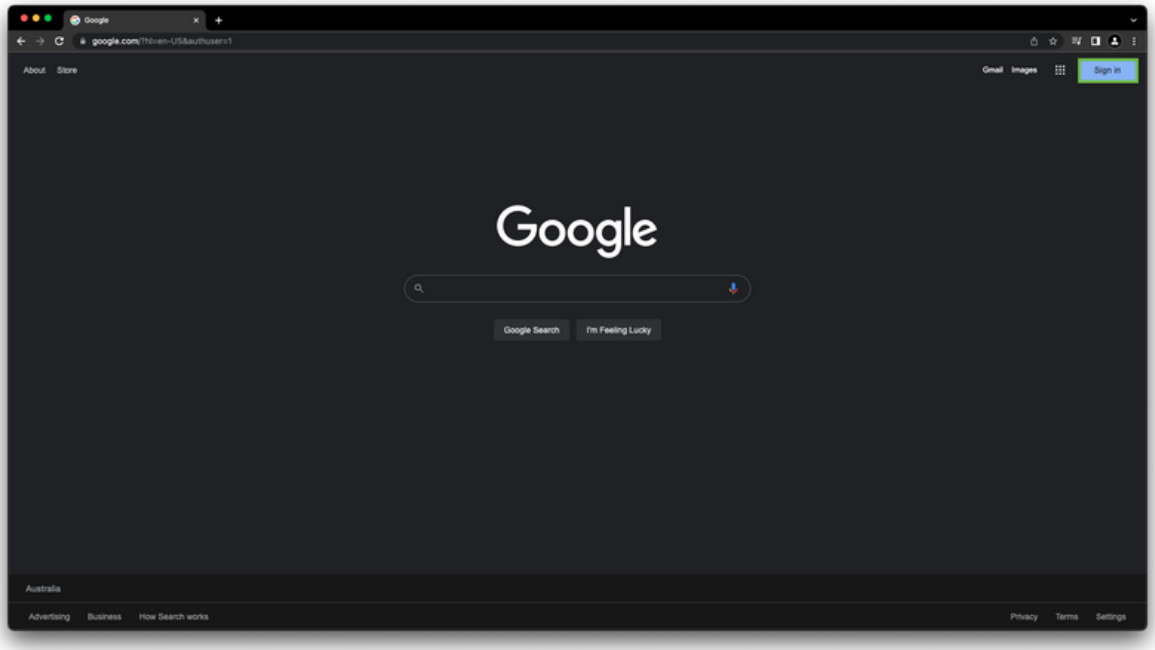
This could be a security code from an authenticator app, SMS, or phone call. Alternatively, you could get a notification to the Google app on your smartphone.

MFA makes it harder for cybercriminals to access your account and it could also alert you to any suspicious activity. This means if your password is guessed or stolen and a cybercriminal is trying to login to your account, you will be sent a security code or notification.

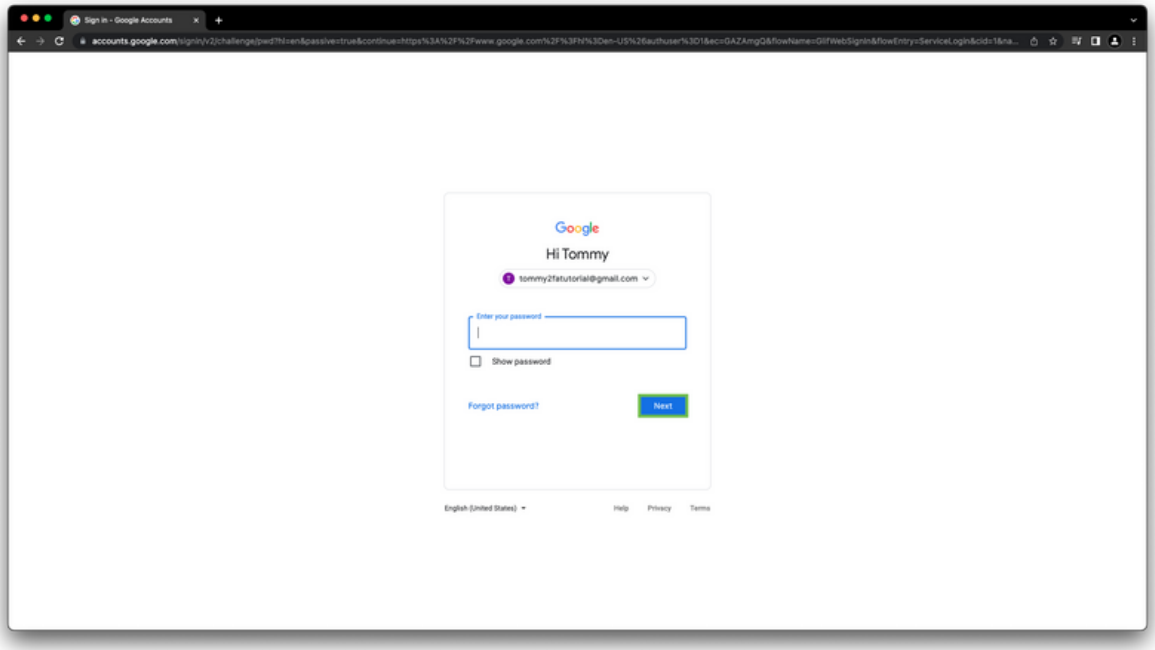
This will prevent them from logging in to your account as they won't have the security code, or you can deny them entry if you use the Google app. You can then change your password to secure your account. If you don't have MFA turned on, you may not get notifications on attempts to log in to your account.

This guide will show you how to set up MFA for your Google Account on your computer. If you don't have access to a computer, you can follow these steps on any device, however some screens may appear different than pictured.

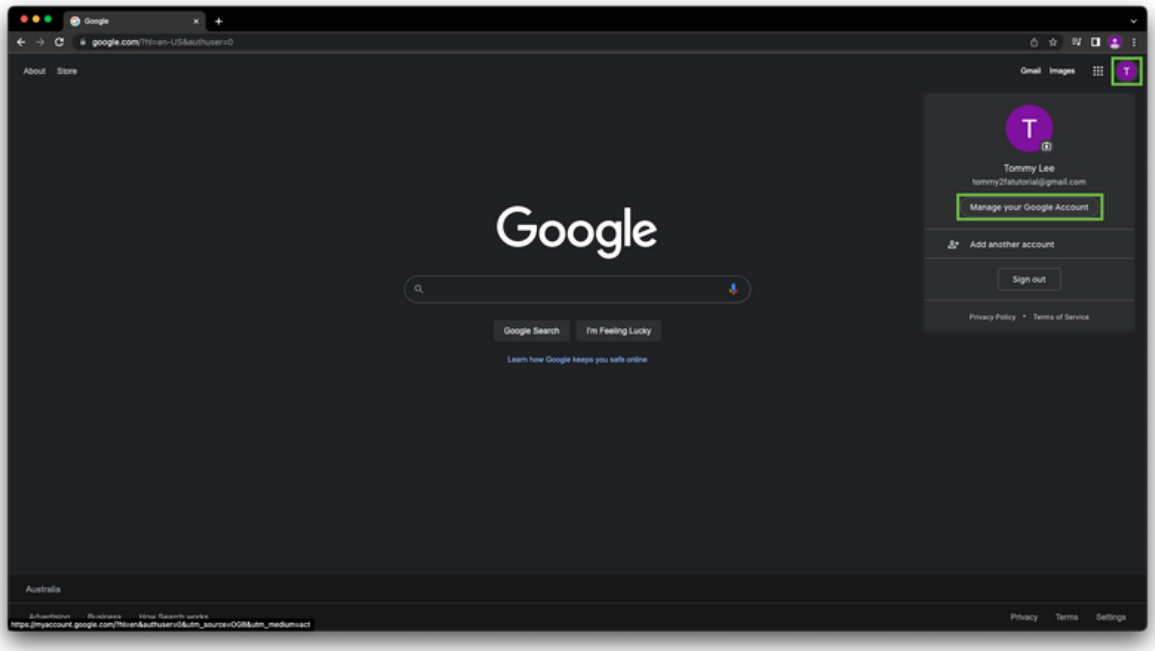
1. Open an internet browser (for example Google Chrome, Microsoft Edge, Mozilla Firefox or Opera). Go to Google (https://google.com.au) and select Sign In in the top right corner.



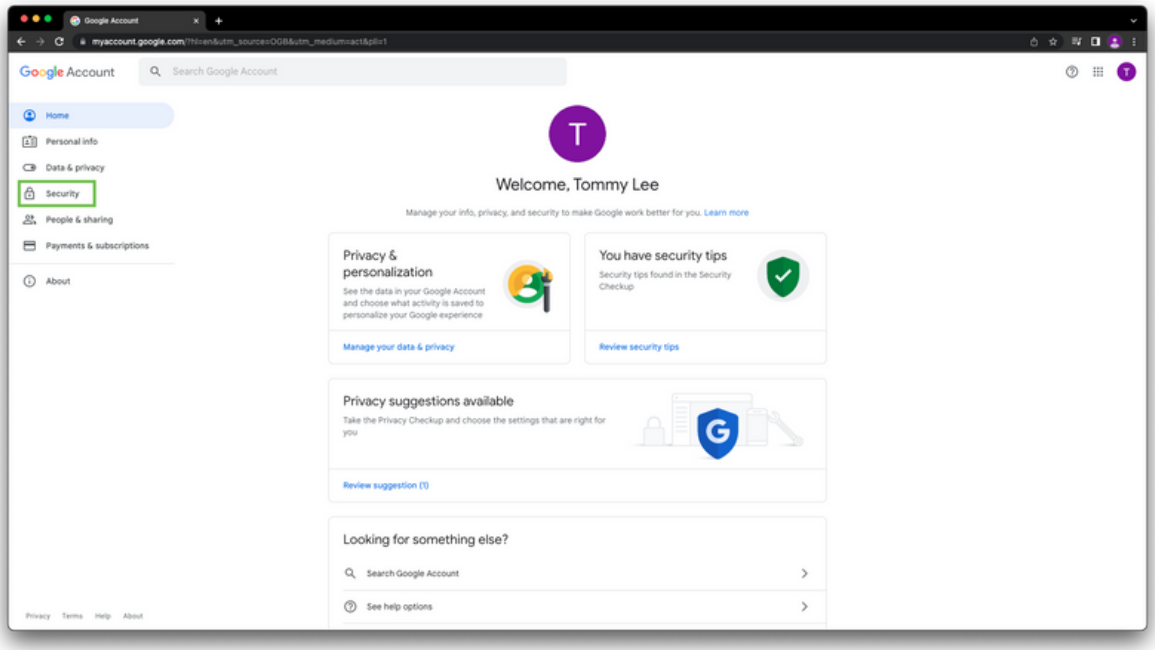
2. Enter your email address and select Next. Then enter your passphrase and select Next.



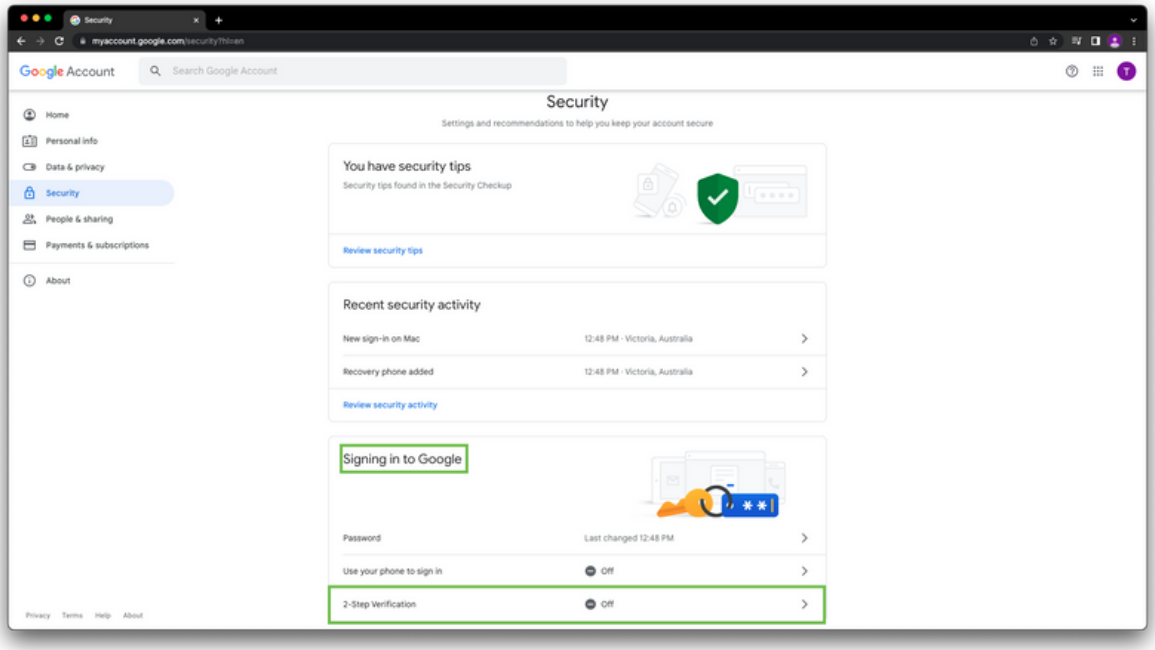
3. Select your user icon in the top right corner. Select Manage your Google Account.



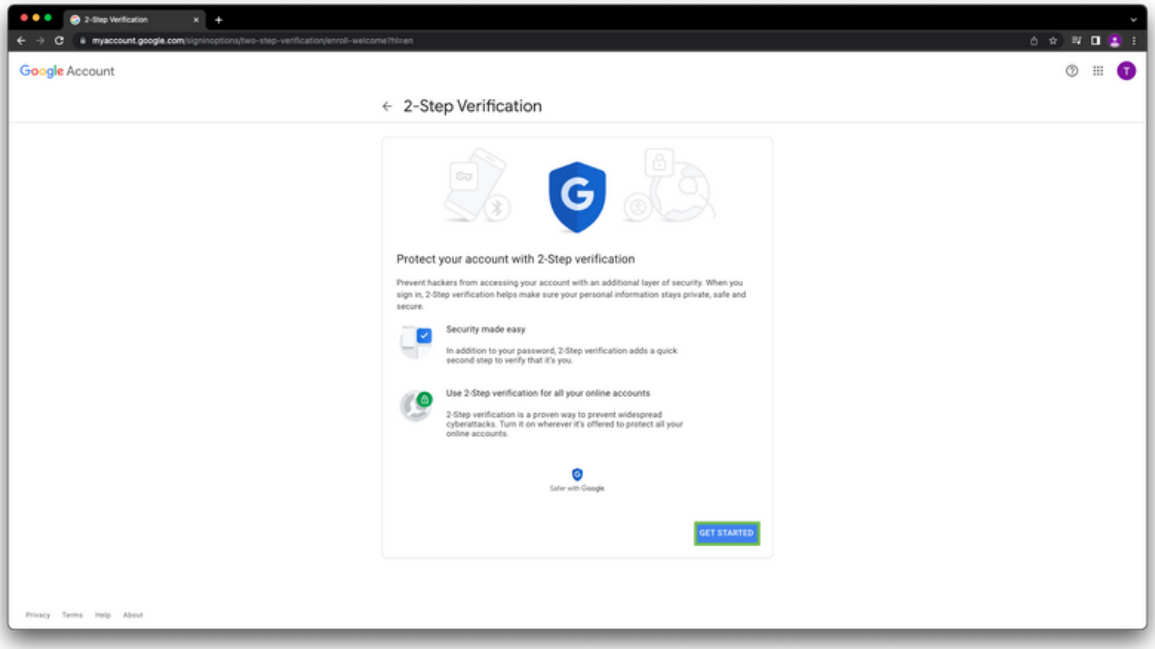
4. Select Security in the list of options on the left of the screen.



5. Under the heading Signing into Google, select 2-Step Verification.

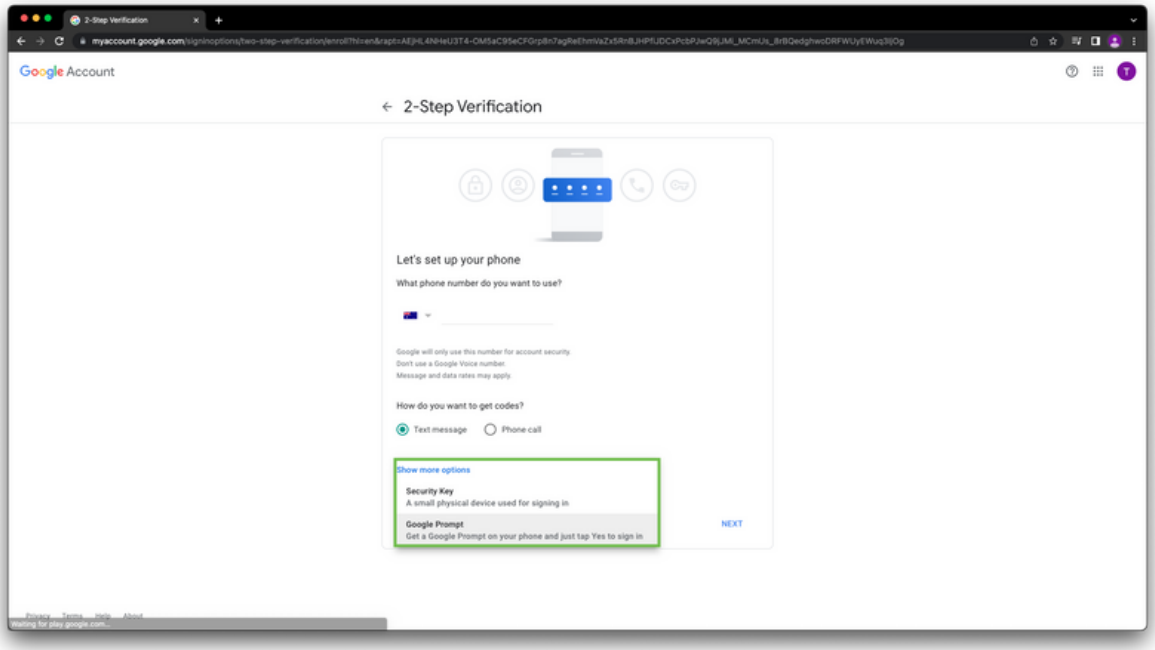


6. Read the information and select Get Started.



7. Re-enter your passphrase and select Next.

8. This is where you will choose how to set up MFA for your Google account. You can either enter your phone number to get security codes via SMS or phone calls, or you can use the Google app. We recommend using the Google app as it is more secure than using a phone number.

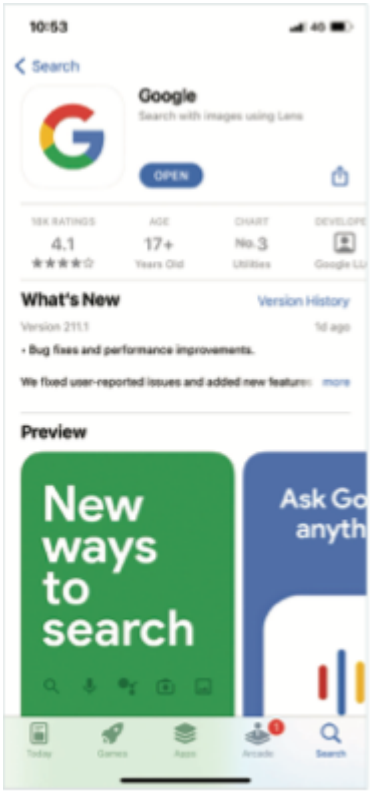


"The Google app will allow you to use your p

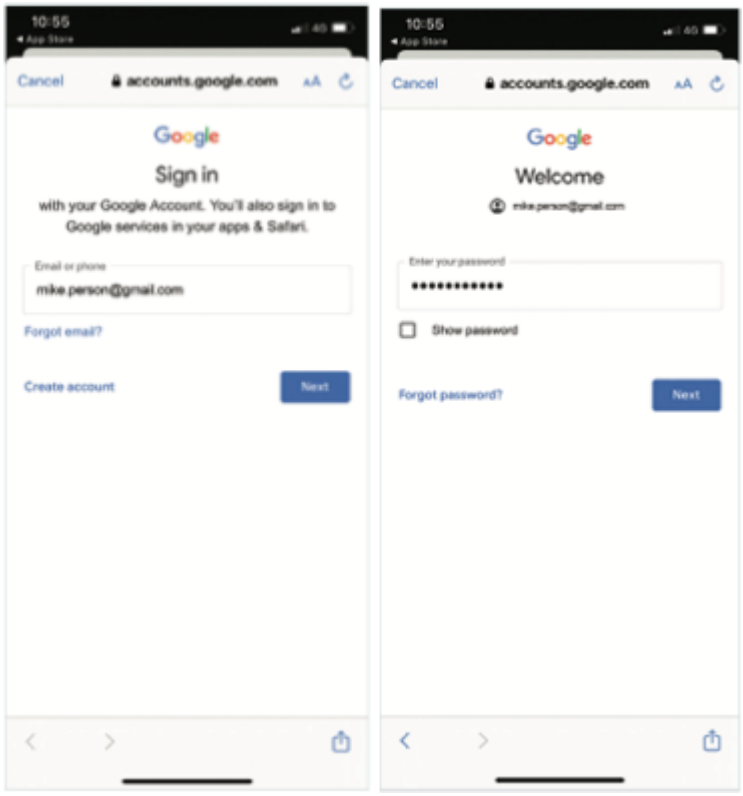
method. That means whenever your Google account is signed in to, you will get a notification on your phone checking whether it is you.
If it is you, you can select Yes to continue signing in.
If it isn't you, then you will know someone has your passphrase and is trying to sign into your account. If this happens, change your passphrase as soon as possible.
If you have not set up your account in the Google app, follow steps 9-11. They show how to set up the Google app on an iPhone, but the steps are similar on Android devices.
If you have already signed into the Google app on your smartphone, skip to Step 12."

9. Go to the App Store or Google Play and search Google.

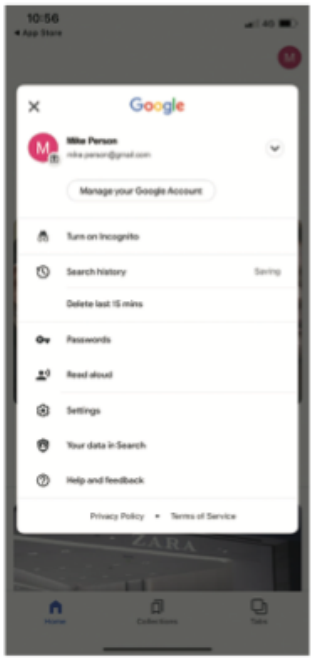
10. Install the Google application and then open it.



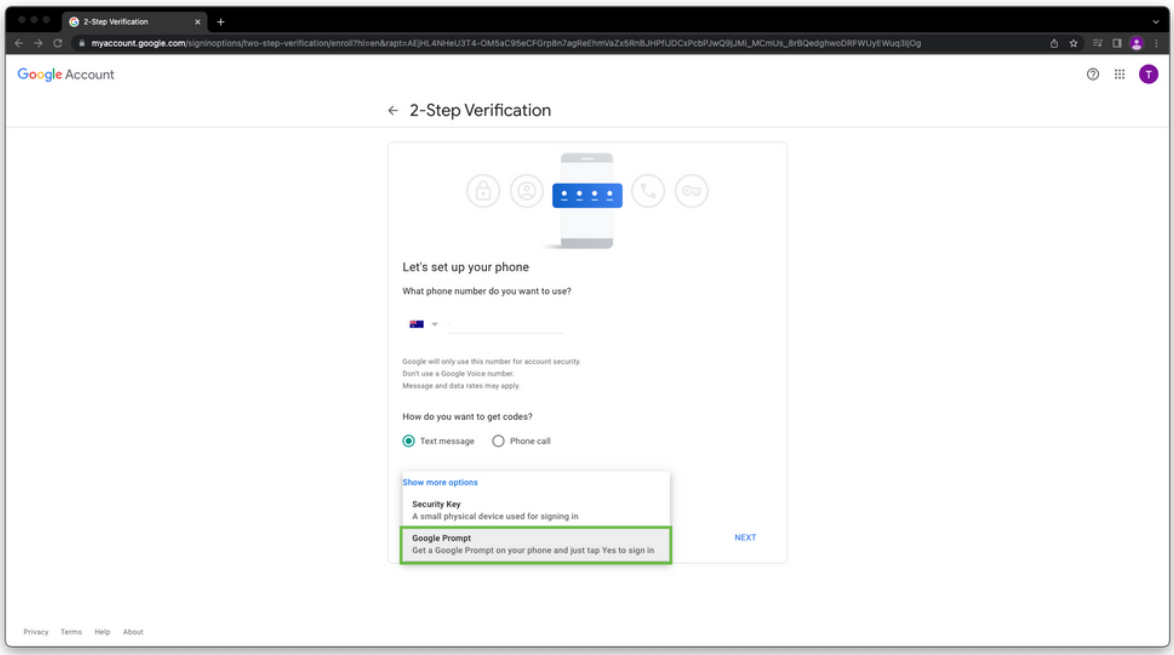
11. Sign in by entering your Enter your passphrase and select Next. Google email address and then select Next.



You will then be signed into the Google application. Follow the rest of the steps in this guide and the Google application will send you a notification whenever you sign into your Google account, asking to confirm if it's you.



12. Now you have signed into the Google application on your phone you will be able to select it to use with MFA. Under Show more options select Google Prompt.



13. Check that you can see your phone and select Continue.

14. Enter your phone number as a backup option in case you can't access your Google application. Select if you would like to receive a Text message or Phone call and then select send.

15. Record your backup codes by downloading them, printing them or writing them down. Make sure you store them in a secure location. Select Next.

16. Select Turn On. Your account will now have MFA enabled.

Additional Security Tips

DO A SECURITY CHECKUP OF YOUR GOOGLE ACCOUNT

Go to the security settings on your Google account to complete a Security check-up. This will give personalised security recommendations for your Google account. You can also review which devices you are signed in on and identify suspicious login activity.

Security Check up (https://myaccount. google.com/security-checkup/2)

USEGOOGLE'S PASSWORD MANAGER

This is a built-in password manager in the Google Chrome browser and Android smartphone operating system. You can save your username and password login credentials for different websites and then automatically fill them in, so you don't have to remember them. This function will also give you the option to generate strong passwords when creating accounts or changing passwords.

For more information see Google's website (https://support.google.com/accounts/ answer/6197437?hl=en)

Third Party 2FA Apps

If you would like to use a third party 2FA app, there are many available. Most are free of charge and effective. Do your research and find a solution that's right for you.

Below are some examples 2FA apps currently available:

Google Authenticator

LastPass Authenticator

Microsoft Authenticator

Authy