Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

# STEP-BY-STEP GUIDE

# CHECK EMAIL ACCOUNT SECURITY GMAIL

cyber.gov.au

# Introduction

**This step-by-step guide will explain how to check the security of your email account for Gmail on your desktop.**

For more information on how to secure your other accounts please see our guides for *Securing Google Accounts* and *Securing Microsoft Accounts*.





Further improve your cyber security with the help of our other guides.

***Personal Cyber Security Series***


***Small Business Cyber Security Guide***


To read the above publications and for other cyber security advice, visit **cyber.gov.au**

## Table of Contents.



# Checking your email account's security

Email accounts are a common target for cybercriminals. If cybercriminals gain access to your email account they can steal your sensitive information, commit fraud or send emails pretending to be you.

Proactively reviewing your email account's security will help you to prevent its compromise and increase your chances of regaining control if it becomes compromised.

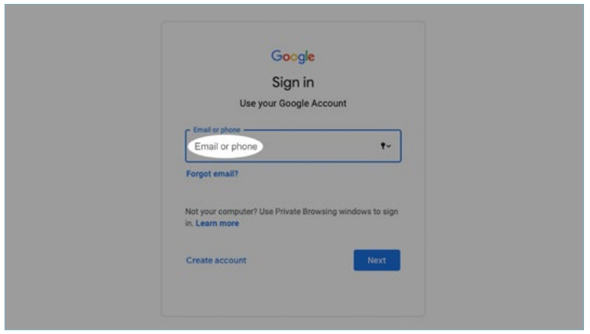




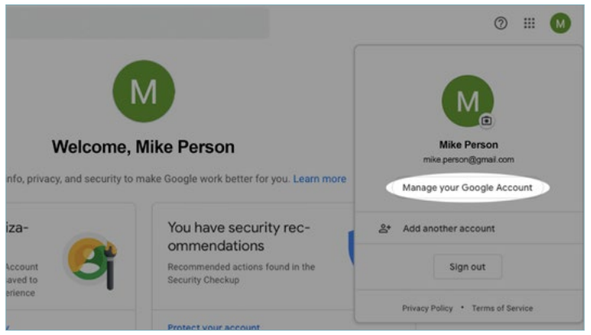

# Step 1: Change your password

If you are concerned that your email account has been hacked, it is important to log in to your account as soon as possible. Once logged in, you can change your password to disrupt a cybercriminal's access and regain control over your email account.

If a cybercriminal has changed your password, skip to Step 1A to recover your email account

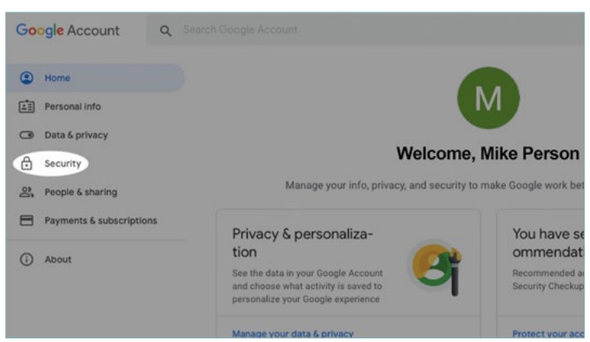



1. Visit **www.gmail.com** and enter your email address.

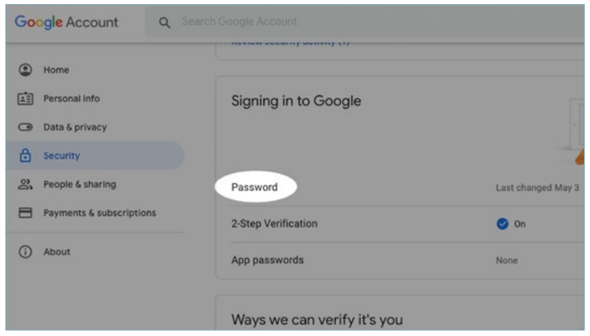



2. Once logged in, select the **Profile** icon (top right) and then select **Manage your Google Account**.

# Step 1: Change your password (cont...)

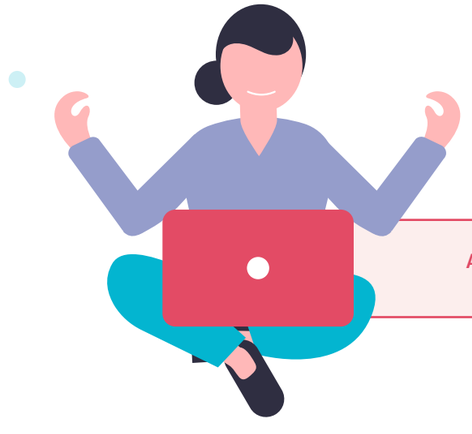



3 From the list on the left side of the screen, select **Security**.




4 Scroll down to the section labelled **Signing in to Google** and select **Password**. Enter your current password and choose a new password.

When choosing a new password, consider creating a passphrase. A passphrase uses four or more random words as your password, which is hard for cybercriminals to guess but easy for you to remember. More information on creating strong passphrases is available from the ACSC. (https://www.cyber.gov.au/acsc/view-all-content/publications/creating-strong-passphrases)



After you have reset your password, skip to **Step 2.**

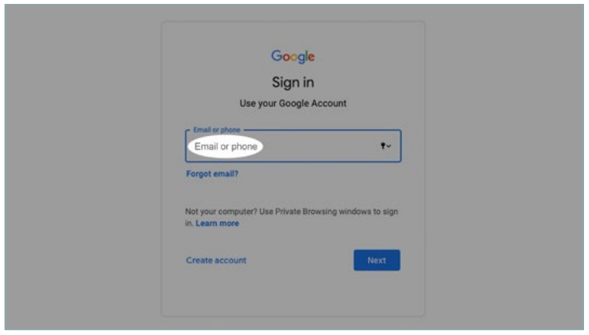




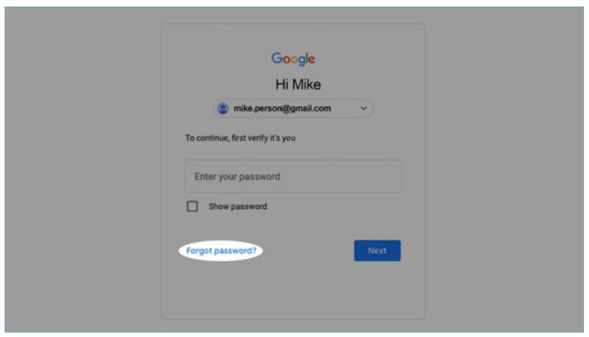
# Step 1A: Recover your email account

Recovery of your email account is only required if a cybercriminal has changed your password. If you have completed the previous step, you can skip this one.

Note that this recovery process will require you to confirm your identity by providing either your phone number or a recovery email address.

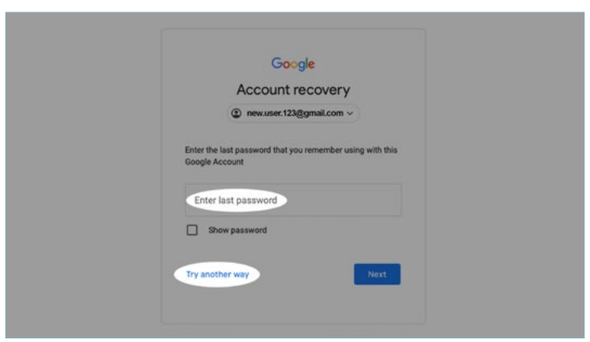



1 Visit **www.gmail.com** and enter your email address.




2 Select **Forgot password?**

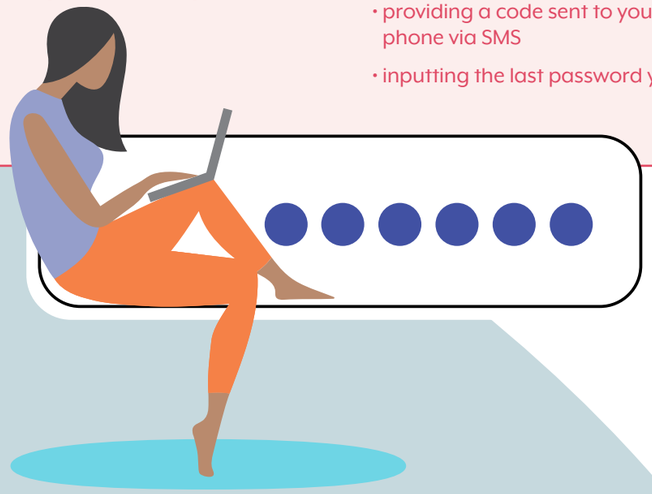
# Step 1A: Recover your email account (cont...)




3 One option to recover your email account is to enter the last password you remember using before your password was changed by a cybercriminal. If you cannot remember your password, select **Try another way**. Carefully follow the recovery process and instructions.

**Please note that this process will be different from person to person depending on what security measures you have set up for your email account. Some recovery methods may include:**

- providing a code from your multi-factor authentication app
- providing a verification code sent to your alternative recovery email address
- providing a code sent to your mobile phone via SMS
- inputting the last password you remember

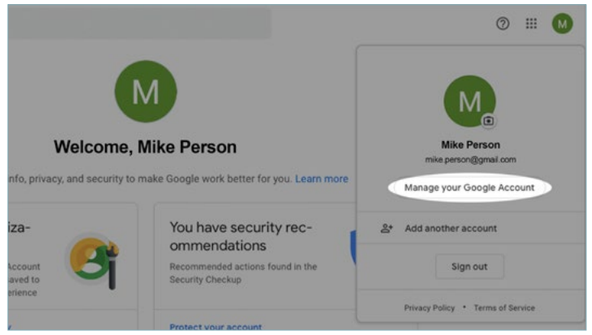




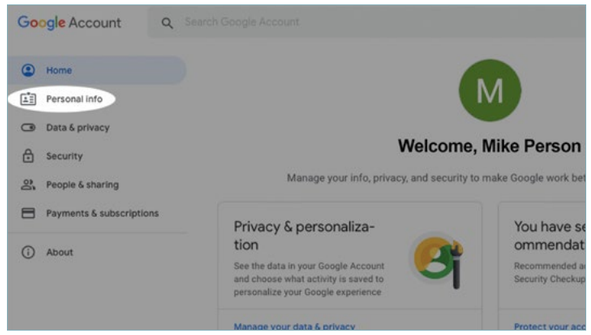


# Step 2: Update your recovery details

In some cases, a cybercriminal may change the recovery details of your email account. They can use this as a way to regain access to the email account even after you have changed your password. Be sure to check your account recovery details are linked to either a recovery email address or recovery mobile phone.

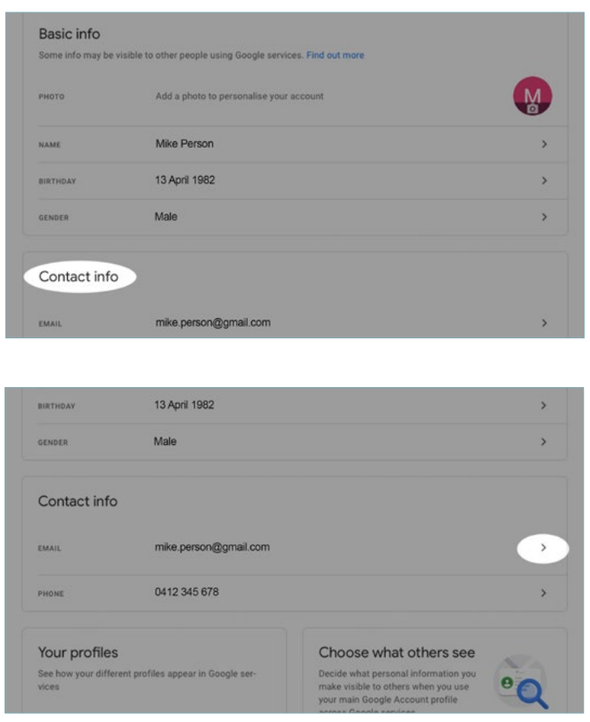



1 From the home screen, select the **Profile** icon (top right) and select **Manage your Google Account**.



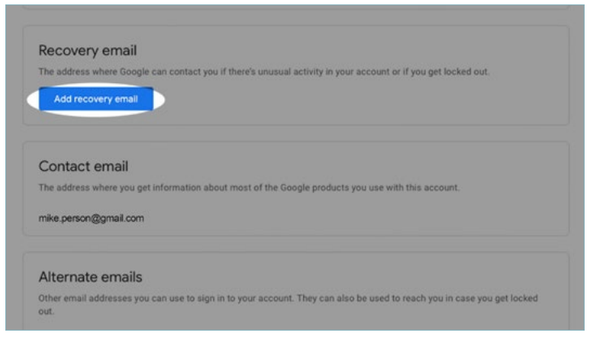

2 From the list on the left side of the screen, select **Personal info**.

# Step 2: Update your recovery details (cont...)




3 Scroll down to the section labelled **Contact info**. You can now change your recovery email and recovery mobile. In doing so, it is important these are changed to email accounts or mobile devices you can access.

4 To change your email, select **Email**.

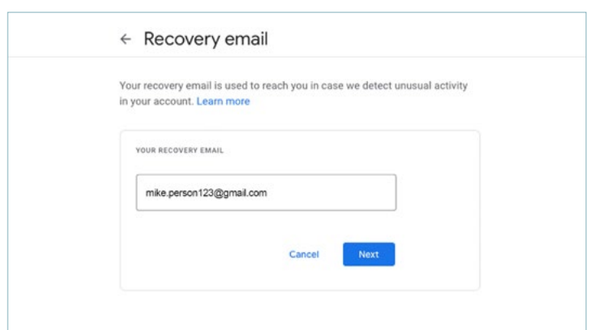



5 Select **Add recovery email**. You will be prompted to re-enter your password.

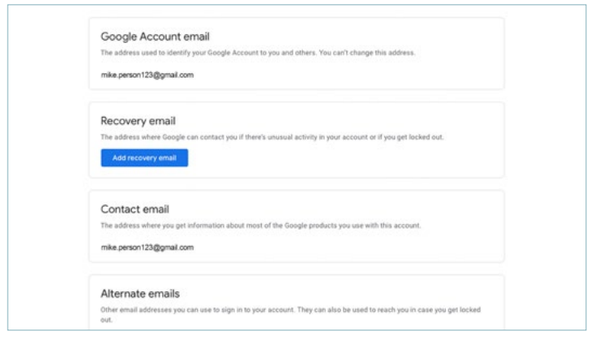




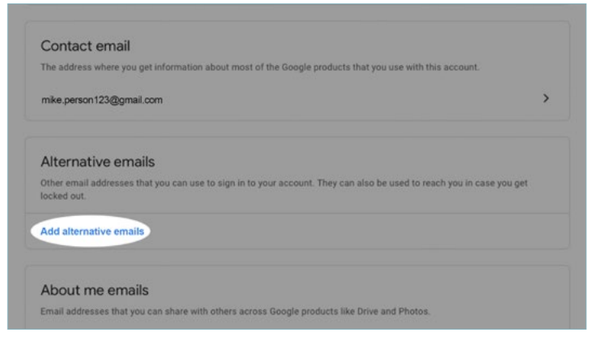
# Step 2: Update your recovery details (cont...)




6 Google will use your recovery email to reach you if unusual activity is detected on your email account or you are accidentally locked out. Select the **pencil icon**. A prompt will open where you can add or update your recovery email.



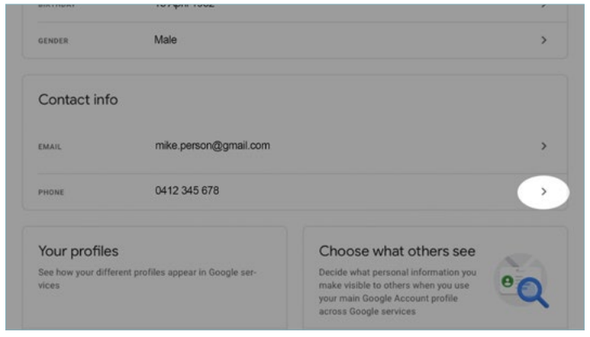

7 Select **Save** to go back to **Email** (Step 4).



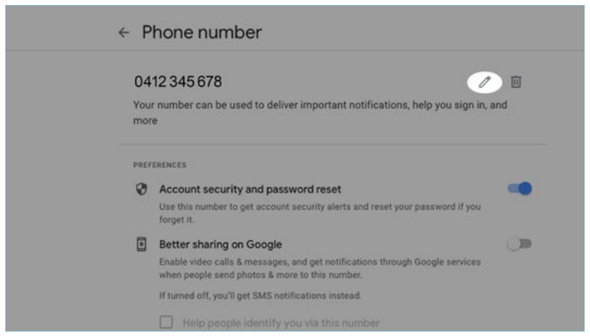

8 From the email options, scroll down to **Alternative emails**. It is important you check no unknown or suspicious email accounts are listed, as a cybercriminal may use these to access your account. If there are email addresses you don't recognise select **Manage alternate emails**.

You will be prompted to re-enter your password. Remove all alternate email accounts to ensure that an alternate account cannot be used to access your account.

# Step 2: Update your recovery details (cont...)




9 To change your phone number, go back to **Personal info** and select **Phone**.




10 Select **Phone** and then the phone number you wish to change. If you have not entered a phone number you can select **Add now** and follow the on screen prompts.

Google will use your recovery phone number to reach you if unusual activity is detected on your email account or you are accidentally locked out. Select the **pencil icon** and re-enter your password.

A prompt will open where you can update your phone number.





# Step 3: Sign out of other sessions

Cybercriminals may still be logged into your email account after you have regained access. By signing out of all sessions you will disrupt a cybercriminal's access and regain control over your email account.

To sign out of all sessions, you will need to change your password. If you have already changed your password in Step 1, then you have already completed this step.

If you have not yet changed your password, instructions on how to do this can be found in Step 1.

# Step 4: Enable Multi-factor Authentication

Turning on multi-factor authentication is the most important defence against cybercriminals gaining access to your email account.

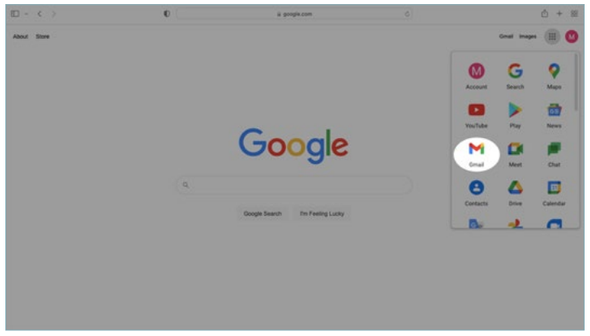
Multi-factor authentication makes it harder for cybercriminals to gain access to your email account by making them guess two pieces of information rather than one (such as a password and a constantly changing PIN).


**For a more detailed set of instructions, see the ACSC's Protect Yourself guide**

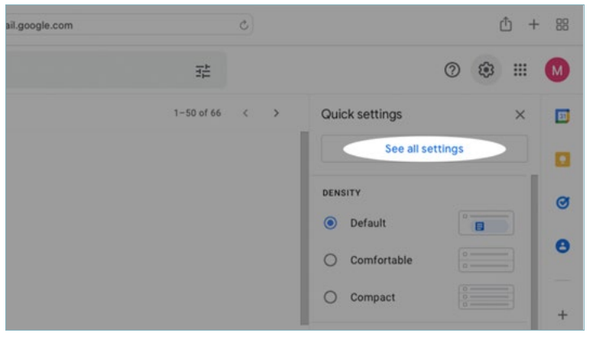
cyber.gov.au/protect-yourself/resources-protect-yourself/personal-security-guides/protect-yourself-multi-factor-

# Step 5: Check account mail settings

Cybercriminals will sometimes set up ‘forwarding rules’ to send themselves a copy of emails coming into or leaving your email account. You should check your email account to see if cybercriminals have set up forwarding rules and delete any you don’t recognise.




1. Log in to your Google account. Select the **Google apps** button and select **Gmail**.

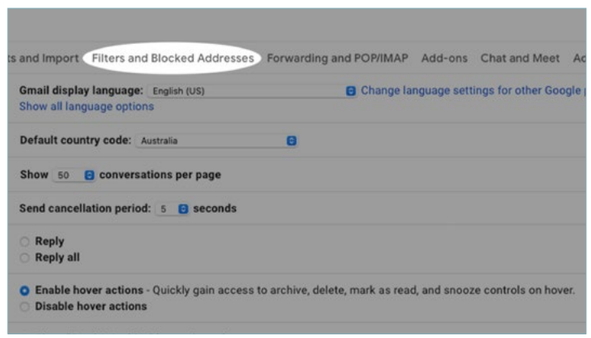



2. From your email account, select the **Settings icon** (cog) and select **See all settings**.

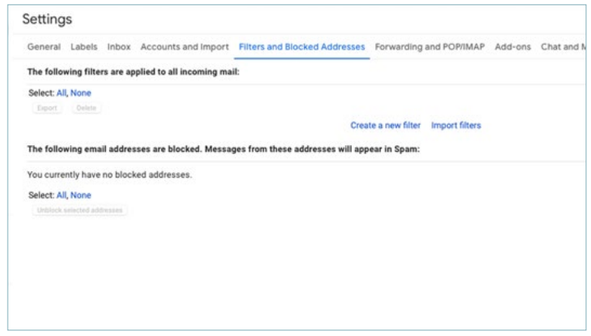




# Step 5: Check account mail settings (cont...)

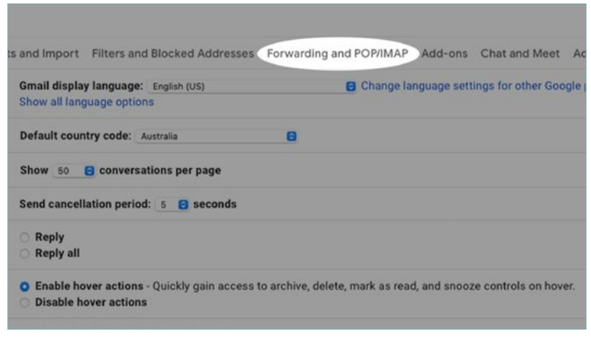



3. From the tabs at the top of the page, select the **Filters and blocked addresses** tab.




4. Check that no unfamiliar filters are being applied to incoming emails, or that there are not any unusual email accounts that are being blocked. Delete any of these unfamiliar filters or email accounts.

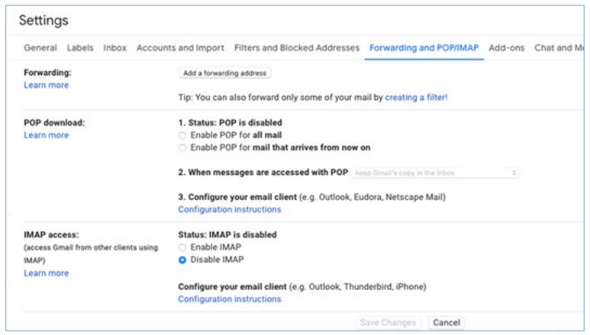
   A cybercriminal may have set these up to hide emails from you, especially if customers or contacts have become suspicious and tried to reach out to you.




5. From the tabs at the top of the page, select the **Forwarding and POP/IMAP** tab.

   POP and IMAP are protocols that allow emails to be accessed through other applications, such as Microsoft Outlook, Apple Mail and Mozilla Thunderbird. Cybercriminals sometimes use these as another method of accessing your email account, as it can allow them to bypass some security measures such as multi-factor authentication.

# Step 5: Check account mail settings (cont...)




6 Make sure there are no forwarding rules, this will prevent cybercriminals who may be forwarding incoming emails. If you don't use an email application and only use a web browser to access your emails, consider disabling POP and IMAP as these can be used by cybercriminals to access your emails from another application. Select **Save changes** when finished.

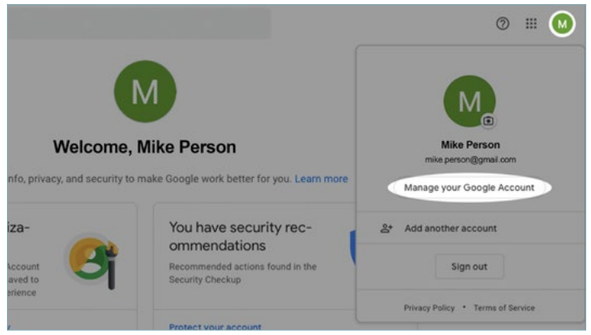




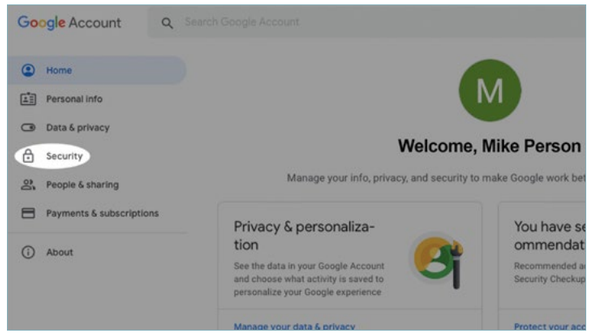

# Step 6: Check third party application access

Have you ever logged into another application or website using your email account, sometimes without needing to put in your password? Many websites and applications can use this method to avoid having to create a new user account. However, the connection this creates between your email account and the website/application is a common way for hackers to gain access to your email account.

Check if there are any apps or services that have access to your account and remove any that you don't recognise or no longer require.

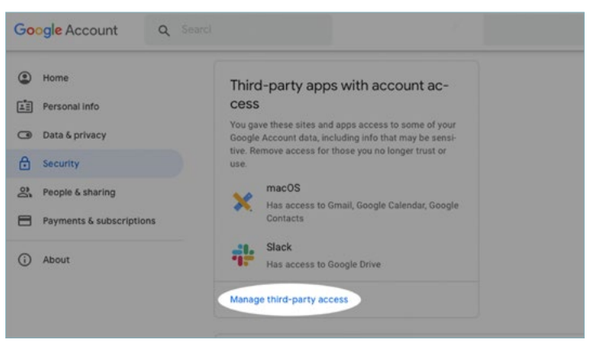



1 From the home screen, select the **Profile** icon (top right) and then select **Manage your Google Account**.

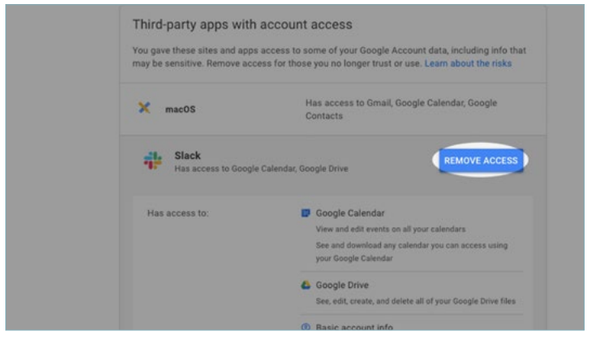



2 From the list on the left side of the screen, select **Security**.

# Step 6: Check third party application access (cont...)

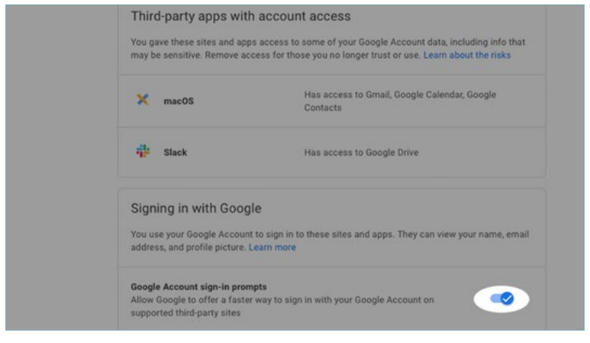



3 Scroll down to Third-party apps with account access and select **Manage third-party access**.




4 It is important to reduce the access by third-party apps to your email account. If a cybercriminal has hacked a third-party app, they may be able to use it to enter your email account.

Select **Remove Access** for each app listed that you didn't configure yourself. If you're not sure what apps might be, remove those you're not sure about as they can be reconfigured later if required.



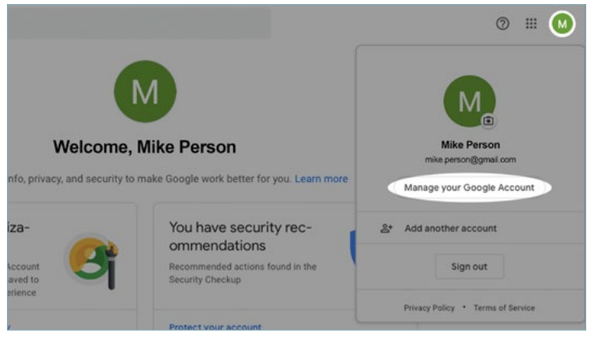

5 Scroll down and select **Google Account sign-in prompts** to ensure the toggle is turned off. This will disable the ability to sign in to third party applications using your Google account.



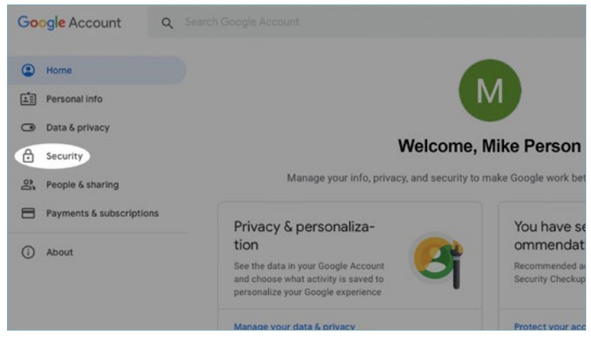


# Step 7: Check login activity

You can see what devices have been used to log in to your account, the time and date they logged in and an estimation of the location where your account was logged in to. As a good practice, regularly review your login activity to check if your email account has been accessed at unusual times or from unusual locations. By doing so, you will be able to pick up on anything suspicious.

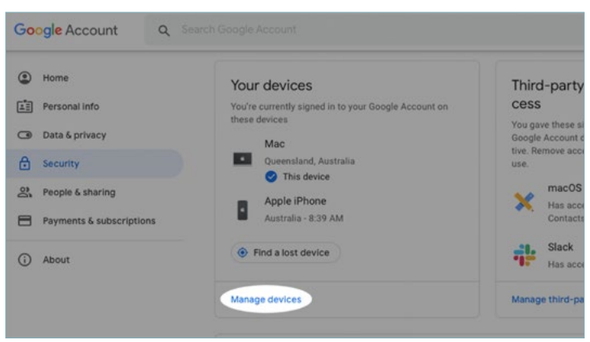



1 From the home screen, select the **Profile** icon (top right) and then select **Manage your Google Account**.

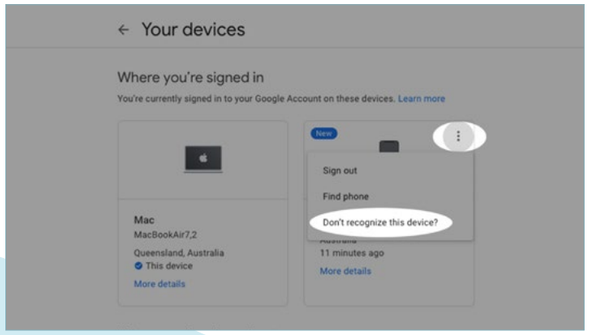



2 From the list on the left side of the screen, select **Security**.

# Step 7: Check login activity (cont...)



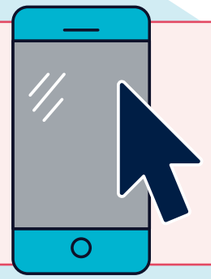

3 Scroll down to Your Devices and select **Manage Devices**.




4 Check the devices you have logged in to. If you see any suspicious activity since the last time you changed your password, change your password immediately. Alternatively can also select **Don't recognise this device** and use Google's security check-up to change your password.

If you have recently changed your password, you will have been signed out of all sessions except the one you used to change your password. You can check all the devices that have been signed out by scrolling down to **Where you've signed out**.

**Here are some things to consider to help you identify suspicious activity:**



- **The Access Type** – is this a device/browser/application you are familiar with, use or own?
- **The Location (IP address)** – was the login from a country you are familiar with?
- **The Date/Time** – does the login date and time seem out of the ordinary?

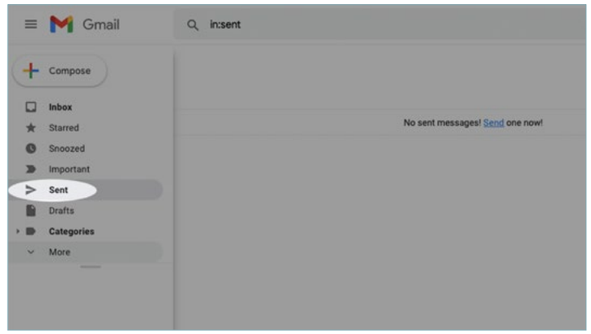




# Step 8: Determine the impact of unauthorised access to your email account

Once you have made sure cybercriminals don't have access to your email account, you may want to consider checking your email folders, specifically your Sent, Draft and Trash folders. This will help you assess what actions a cybercriminal may have taken when they accessed your email account.

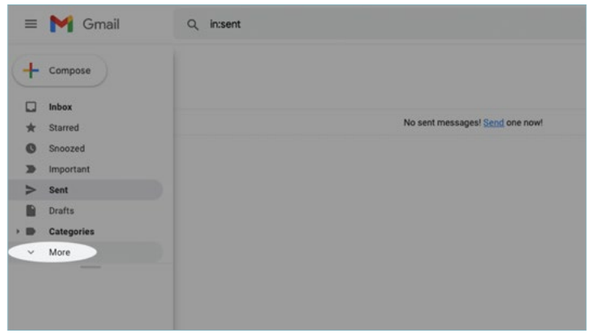
If someone has hacked into your email account, they may have tried to reset passwords for other online accounts that are linked to that email address. These could be for banking and finance, social media, or other accounts. Check for any password reset emails.




1 From your inbox, select **Sent** to view your sent emails.

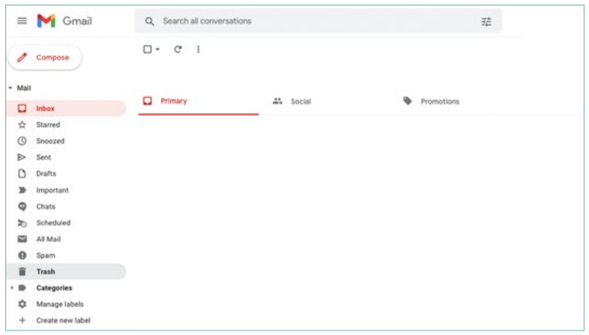
Search for emails that you did not send and take note of the recipient, whether attachments were included, what the email was requesting and when it was sent.

Compare any unusual activity times with the time the email was sent. **Verify login records** to confirm that a criminal contacted someone from your email account.

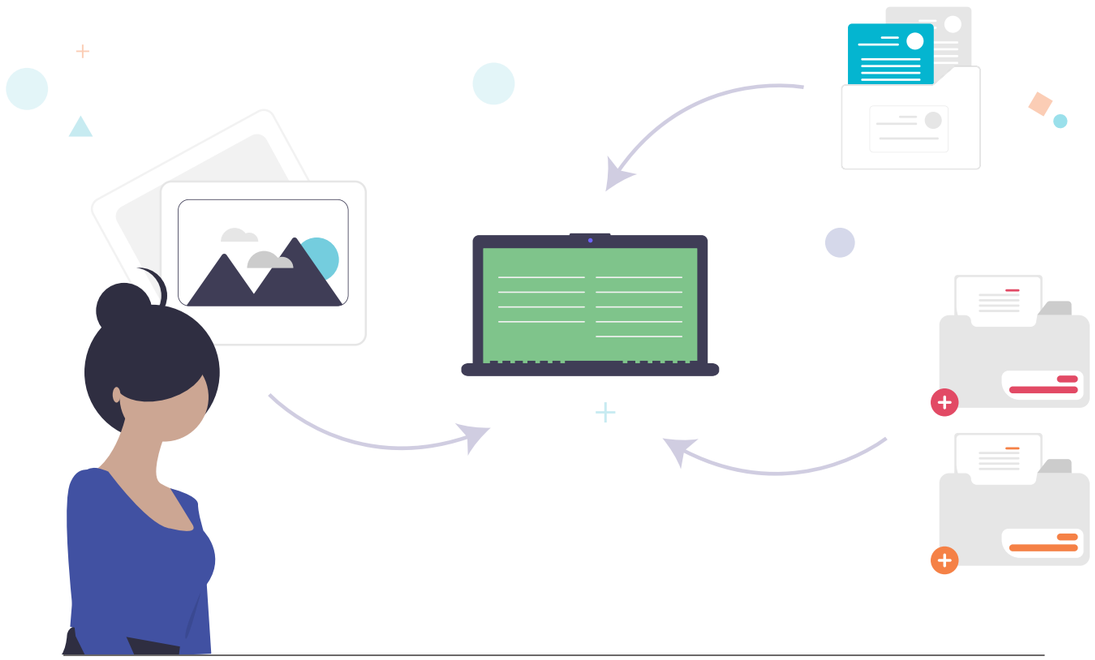



2 Under the Sent folder on the right, select **More** to make more folders visible.

# Step 8: Determine the impact of unauthorised access to your email account (cont...)




3 Undertake the same steps taken for your other folders, especially **Drafts** and **Trash** folders.







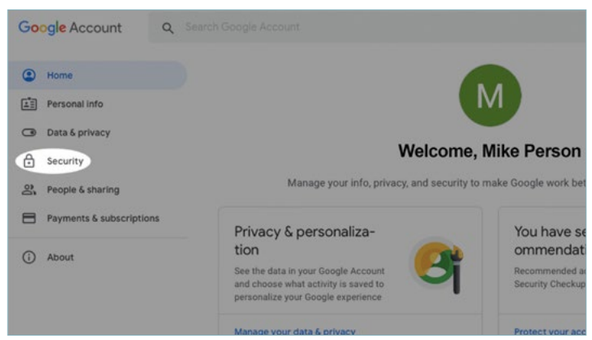
# Step 9: Enable Enhanced Safe Browsing

Enhanced safe browsing is a tool that will warn you about risky downloads, sites and extensions. It will also warn you about potential password breaches and send additional data to Google about your activity.

More information on Google Enhanced safe browsing can be found on their website. (https://support.google.com/chrome/answer/9890866?hl=en&co=GENIE.Platform%3DAndroid)

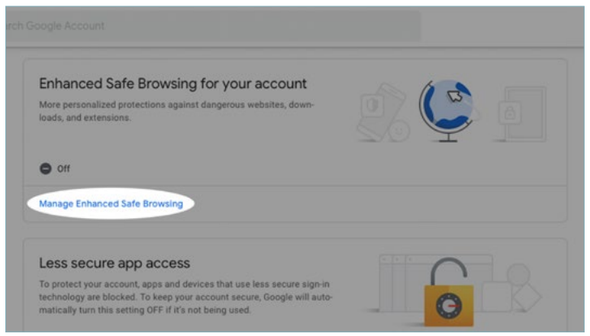



1 **Profile icon** (top right) and then select Manage your **Google Account**.

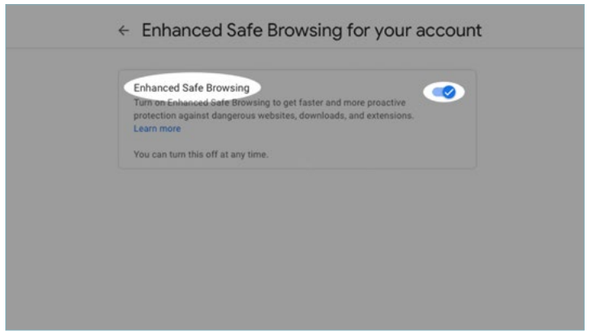



2 From the list on the left side of the screen, select **Security**.

# Step 9: Enable Enhanced Safe Browsing (cont...)




3 Scroll down to Enhanced safe Browsing for your account and select **Manage Enhanced Safe Browsing**.




4 Toggle **Enhanced Safe Browsing**, read the information and follow the prompt to turn on.





# Security Tips

## Check saved passwords

Have you ever saved your passwords using your web browser? If you were signed in to a Chrome web browser and saved your username and password then those credentials can be accessed from your Google account.
If a cybercriminal has accessed your account, they may have also accessed your saved passwords. We recommend changing any saved account passwords that are stored on your Google account.

## Check other accounts

If you used the same password for your email account and any other accounts, these may be no longer secure. You should complete the following steps to help keep your other accounts secure:

- Change the password on accounts that shared the same password.
- Enable multi-factor authentication where possible on these accounts.
- Change the passwords to unique strong passphrases if multi-factor authentication isn't available.

## Use a password manager

Password managers (which can also be used to store passphrases as well) enable good cyber security habits. Having a unique passphrase for every valuable account may sound overwhelming; however, using a password manager to save your passphrases will free you of the burden of remembering which passphrase goes where.

A lot of web browsers provide an in-built password manager. You might have noticed the pop-up window asking to store your password when logging into accounts. Password managers are also sold separately, however, quality and security may vary.

When using a password manager:

- conduct research to ensure the password manager is from a reputable vendor
- conduct research to ensure the password manager is maintained by the vendor with regular security updates
- protect the password manager with its own strong and memorable passphrase.

You may choose to keep track of your passphrases in a notebook rather than a password manager. No matter how you keep track of your passphrases, ensure you have a secure storage method.

# Notes



Check Email Account Security - **Gmail**

# Notes

**Disclaimer**

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.



**For more information, or to report a cyber security incident, contact us:**

cyber.gov.au | 1300 CYBER1 (1300 292 371)