Australian Government
Australian Signals Directorate

Australian
Cyber Security
Centre

Step-by-Step Guide

Check Email Account Security

Outlook, Microsoft 365, Live, Hotmail & MSN

cyber.gov.au

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.

Copyright

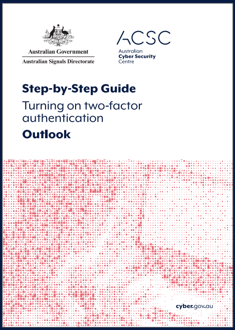
Use of the Coat of Arms

Table of Contents

Introduction

This step-by-step guide will explain how to check the security of your email account for **Outlook.com, Microsoft 365, Live, Hotmail, and MSN** on your desktop.

Other step-by-step guides include:

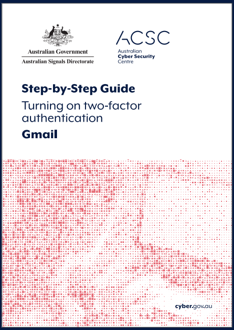


Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Step-by-Step Guide
Turning on two-factor authentication
Outlook

cyber.gov.au

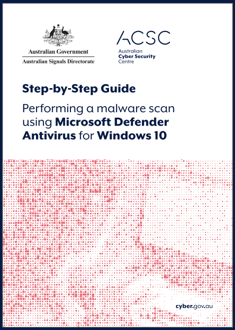


Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Step-by-Step Guide
Turning on two-factor authentication
Gmail

cyber.gov.au

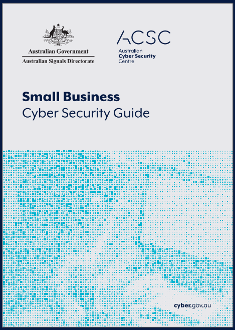


Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Step-by-Step Guide
Performing a malware scan using **Microsoft Defender Antivirus** for **Windows 10**

cyber.gov.au

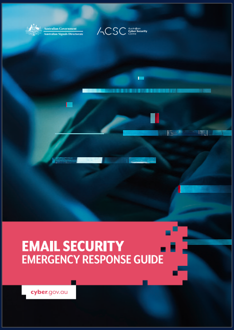


Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Small Business
Cyber Security Guide

cyber.gov.au

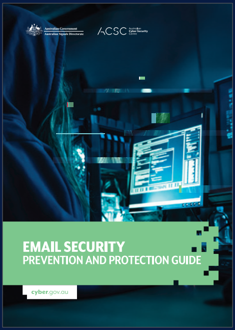


Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

EMAIL SECURITY
EMERGENCY RESPONSE GUIDE

cyber.gov.au



Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

EMAIL SECURITY
PREVENTION AND PROTECTION GUIDE

cyber.gov.au

For more cyber security advice, visit **cyber.gov.au**

Checking your email account security

Email is a common target for cybercriminal activity. If someone gains unauthorised access to your email account, they can access your private communications. A cybercriminal could steal your sensitive information, or even commit fraud and send emails pretending to be you.

After any email security incident you should review the security on your account, even if you are not sure that you have been hacked.

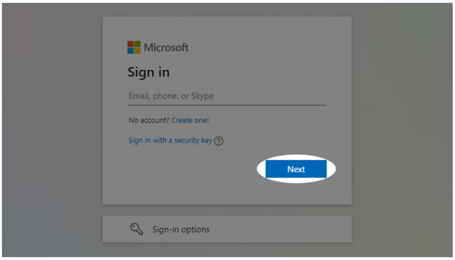
Reviewing your account security will help you to identify intruders, regain control of your account, and help prevent cyber attacks in the future.

Step 1: Change your password

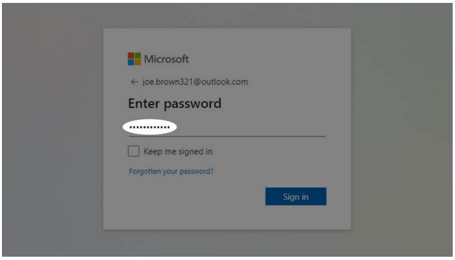
If you are concerned that your email account has been hacked, it is important to login to your account as soon as possible. Once logged in, you will be able to disrupt the hacker's access and regain control of your account.

If you have forgotten your email password, please skip to Step 1A to recover your account.

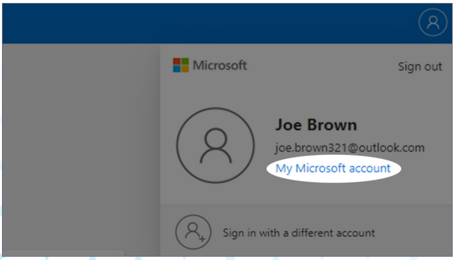
Changing your password is important when investigating the security of your email account. If a hacker knows your password, changing your password will slow them down and make it harder for them to get access to your account.



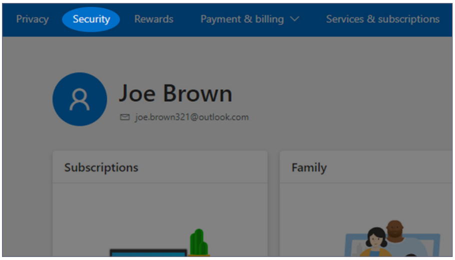
1. Visit **https://account.microsoft.com** and enter your email address and click **Next**.



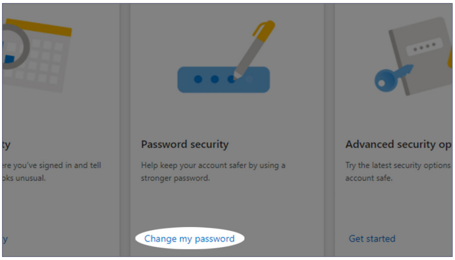
2. Enter your password.



3. Once logged in, click on **Profile** icon (top right) and then click on **My Microsoft Account** or **My Account**.



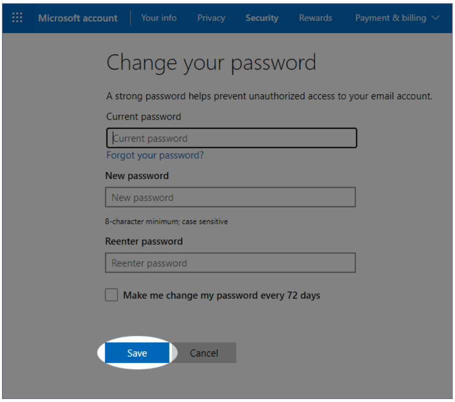
4. On the top menu bar, click on **Security**.



Help keep your account safer by using a stronger password.

Try the latest security options account safe.

5. Under Security Basics, on the **Password Security** tile, click on **Change my password**.



Change your password

A strong password helps prevent unauthorized access to your email account.

Current password

Current password

Forgot your password?

New password

New password

8-character minimum; case sensitive

Reenter password

Reenter password

□ Make me change my password every 72 days

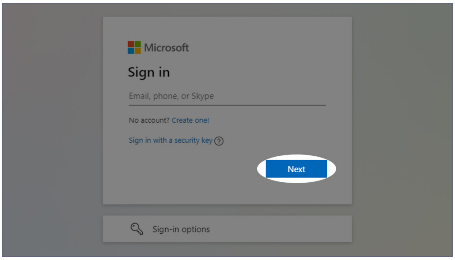
6. Enter your current password, your new password, confirm and click **Save**. By changing your password, all other sessions will be prompted for the new password. However, this does take a few minutes.

   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 hack but easy for you to remember.

   Find more information on creating unique strong passphrases at **cyber.gov.au**.

Step 1A: Recover your account

Recovery of your account is only required if you do not remember your email password. Note that this recovery process will require you to confirm your identity by providing either your phone number or recovery email address.

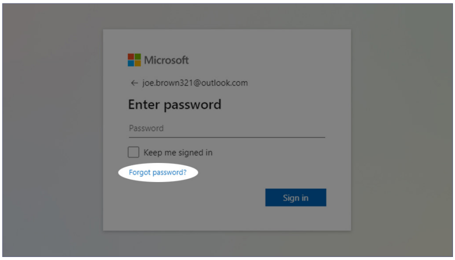


Email, phone, or Skype

No account? Create one!

Sign in with a security key

1. Visit **https://account.microsoft.com** and enter your email address and click **Next**.

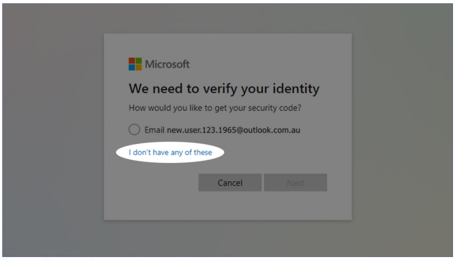


joe.brown321@outlook.com

Password

□ Keep me signed in

2. Click **Forgot password**.

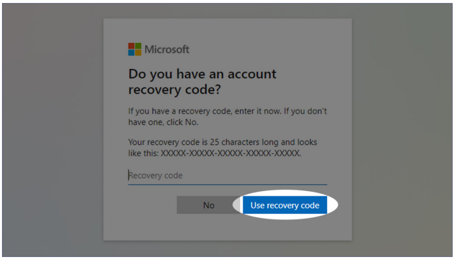


How would you like to get your security code?

○ Email new.user.123.1965@outlook.com.au

3. If you have access to an external **Email** or **Mobile** phone to receive the recovery code, click on the appropriate method and proceed to Step 4 of 1A.

   If you don't have access to any of these click on **I don't have any of these** and proceed to Step 5 of 1A.



Microsoft

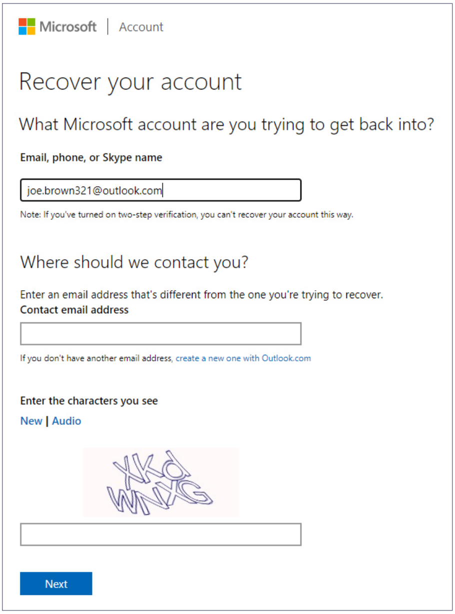
Do you have an account recovery code?

If you have a recovery code, enter it now. If you don't have one, click No.

Your recovery code is 25 characters long and looks like this: XXXXX-XXXXX-XXXXX-XXXXX-XXXXX.

Recovery code

4. If you have a recovery code, enter it and click **Use recovery code**. Proceed to Step 2: Update your account recovery details (page 10).



Microsoft | Account

Recover your account

What Microsoft account are you trying to get back into?

Email, phone, or Skype name

joe.brown321@outlook.com

Note: If you've turned on two-step verification, you can't recover your account this way.

Where should we contact you?

Enter an email address that's different from the one you're trying to recover.

Contact email address

If you don't have another email address, create a new one with Outlook.com

Enter the characters you see

5. If you do not have any recovery accounts of a recovery code, click on **No** which will begin the application process to recover your email address.

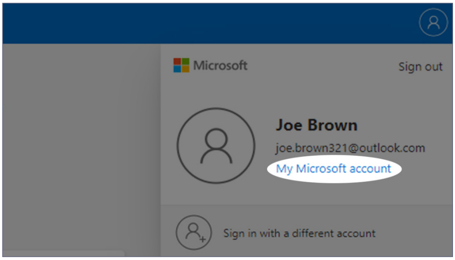
   You may be required to provide an alternative email address to which a recovery code/email will be sent to and to complete an audio or visual CAPTCHA.

   Provide as much information as possible as this will help you recover your account.

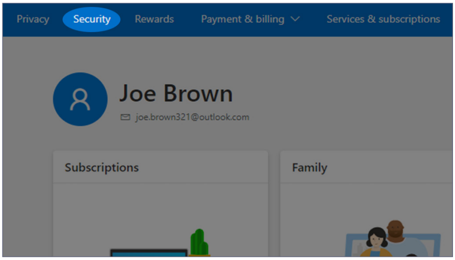
   It may take several days or weeks to receive an outcome as your request is reviewed.

Step 2: Update your account recovery details

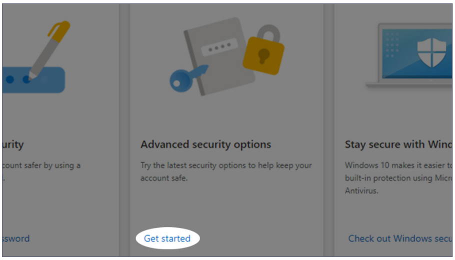
In some cases, a cybercriminal might change the recovery details of hacked accounts. They can use this as a back door to regain access to the hacked account even after you have changed your password. Be sure to check your account recovery details are linked to either a recovery email address or recovery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



1. Click on your Profile in the top right corner and click on **My Microsoft Account** or **My Account**.



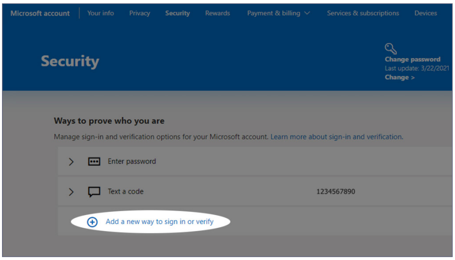
2. Click on **Security** in the Top menu bar. You may have to enter your password again to verify you can make changes to sensitive info.



Try the latest security options to help keep your account safe.

Windows 10 makes it easier to built-in protection using Micr Antivirus.

3. Under Security Basics, on the **Advanced security options** or **Security contact info** tile, click **Get started** or **Update my info**.



Manage sign-in and verification options for your Microsoft account. Learn more about sign-in and verification.

4. Review the recovery details and click **Remove** for any security contact info you want to remove.

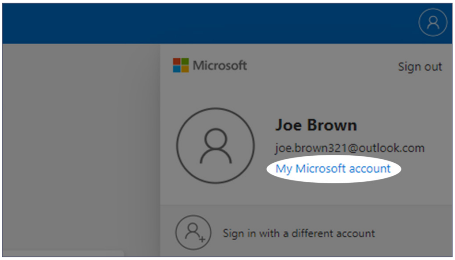
   Note – if only one recovery mechanism is listed, and it is the one you want to delete, you will need to add a valid recovery mechanism first.

   To do this click **Add Security info**.

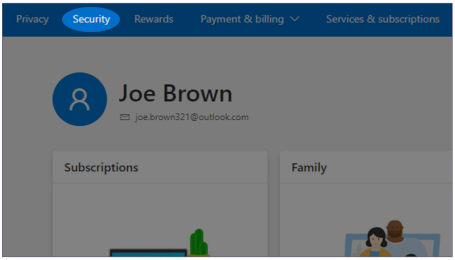
   For Outlook this can either can be a mobile number or an alternative email address.

Step 3: Sign out of all other sessions

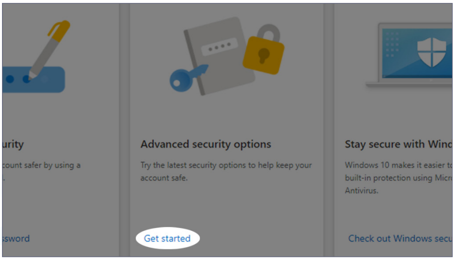
Cybercriminals may be logged in to your email account. By signing out of all sessions, you will remove the cybercriminal's access to your emails.



1. Click on your **Profile** icon in the top right corner and click on **My Microsoft Account** or **My Account**.



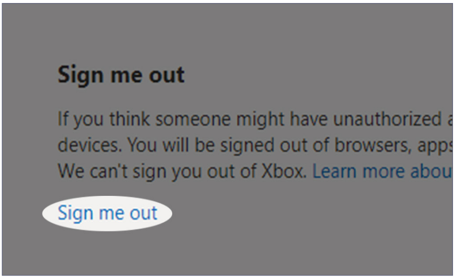
2. Click on **Security** in the top menu bar. You may have to enter your password again to verify you can make changes to sensitive info.



Try the latest security options to help keep your account safe.

Windows 10 makes it easier t
built-in protection using Micr
Antivirus.

3. Under Security Basics, on the **Advanced security options** or **Security contact** info tile, click **Get started** or **Update my info**.



Sign me out

If you think someone might have unauthorized a
devices. You will be signed out of browsers, apps
We can't sign you out of Xbox. Learn more abou

4. Scroll down to **Sign me out** and click on the **Sign me out** button. You will be prompted again to confirm whether or not you want to sign out. Click **Sign me out**.

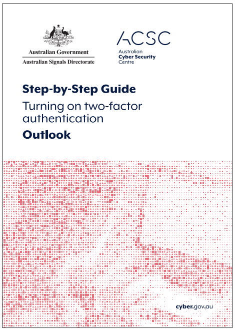
   Note that all account sessions on all browsers and devices will be signed out within 24 hours.

   Once completely signed out of all sessions and devices, sign back in again using your device to continue securing your Microsoft account.

Step 4: Enable multi-factor authentication

Turning on multi-factor authentication (MFA) is the most important defence against hackers gaining access to your Microsoft account.

MFA makes it harder for criminals to gain initial access to your device, account and information by making them jump through more security hoops and additional authentication layers, requiring extra time, effort and resources.



Australian Government
Australian Signals Directorate

ACSC
Australian
Cyber Security
Centre

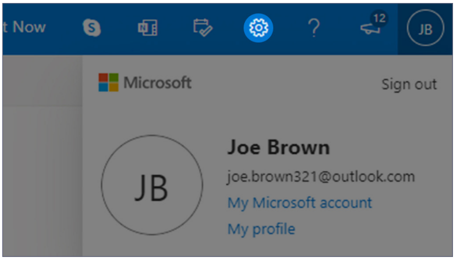
Step-by-Step Guide
Turning on two-factor authentication
Outlook

cyber.gov.au

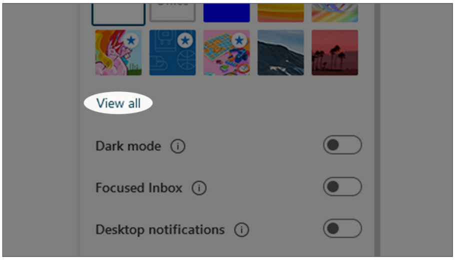
For a more detailed set of instructions, see the ACSC's Step-by-Step guide *Turning on Two-Factor Authentication – Microsoft Accounts* available on **cyber.gov.au**.

Step 5: Check account mail settings

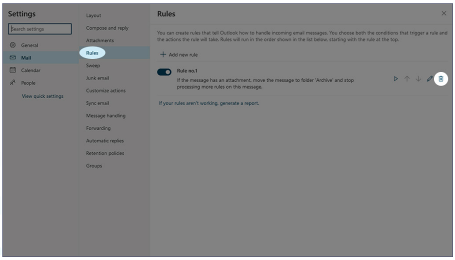
Hackers will sometimes set up forwarding rules to send themselves a copy of emails coming in or leaving your account. You should check your account to see if anyone has set up forwarding rules and delete any you don't recognise.



1. Click on the **Settings** (cog icon) in the top right corner.



2. Scroll down and click on **View all Outlook settings**.



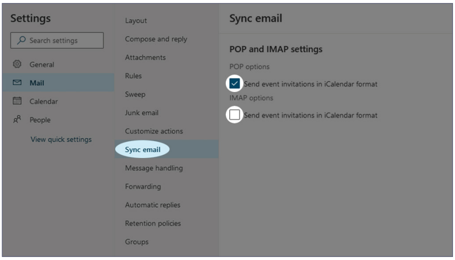
You can create rules that tell Outlook how to handle incoming email messages. You choose both the conditions that trigger a rule and the actions the rule will take. Rules will run in the order shown in the list below, starting with the rule at the top.

If the message has an attachment, move the message to folder 'Archive' and stop processing more rules on this message.

If your rules aren't working, generate a report.

3. In the **Mail** side bar menu, click on **Rules** in the sub-menu and view all the rules.

   To remove any rules, click the **delete icon** (trash icon) and click **OK**.



Sync email

POP and IMAP settings

POP options

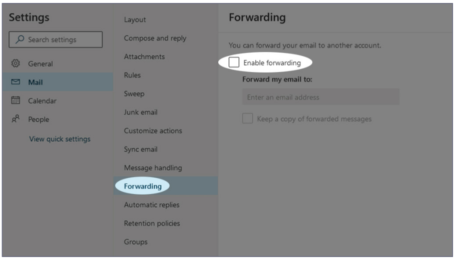
☑ Send event invitations in iCalendar format

IMAP options

□ Send event invitations in iCalendar format

4. Check to see if any of your emails are being accessed by any suspicious external email clients or applications via POP or IMAP1. These are two methods used to access your email externally.

Click on **Sync Email** in the sub-menu and scroll down to view **POP and IMAP**. These should either be disabled or refer to a Server relating to Outlook or Microsoft Office.



Forwarding

You can forward your email to another account.

□ Enable forwarding

Forward my email to:

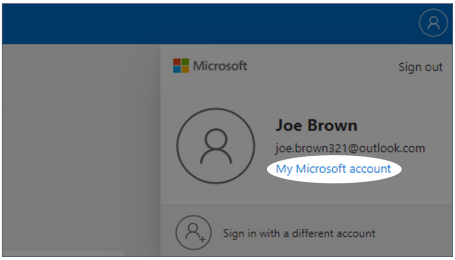
Enter an email address

□ Keep a copy of forwarded messages

5. From here you can check to see if any of your emails are being forwarded to another account.

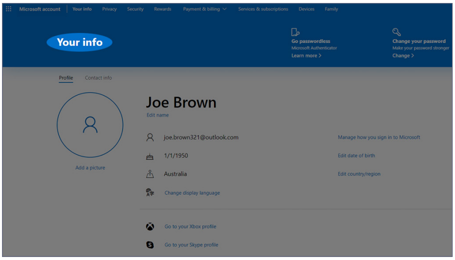
Click on **Forwarding** in the sub-menu, check the **Enable Forwarding** is **unticked**, or if forwarding is turned on, it is to an account you expected.

If forwarding is turned on to an account you don't recognise then turn it off by unticking the box.



6. To use "Manage how you sign in to Microsoft" to see if there are any unusual account aliases still associated to your account, first go to **My Microsoft Account** or **My Account**.

Step 5: Check account mail settings CONT...



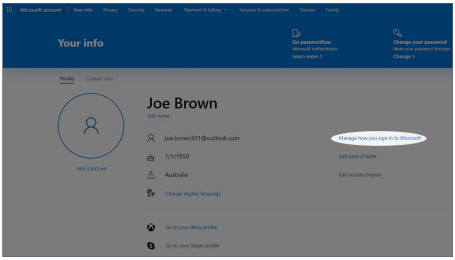
Joe Brown

joe.brown321@outlook.com

1/1/1950

Australia

7. Then click on **Your info**.



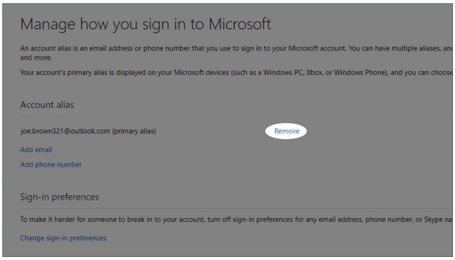
Joe Brown

joe.brown321@outlook.com

1/1/1950

Australia

8. Then go to **Manage how you sign in to Microsoft**.



Manage how you sign in to Microsoft

An account alias is an email address or phone number that you use to sign in to your Microsoft account. You can have multiple aliases, anc and more.

Your account's primary alias is displayed on your Microsoft devices (such as a Windows PC, Xbox, or Windows Phone), and you can choose

Account alias

joe.brown321@outlook.com (primary alias)

Sign-in preferences

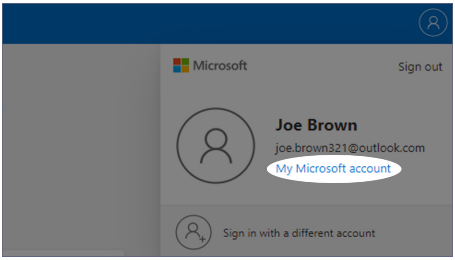
To make it harder for someone to break in to your account, turn off sign-in preferences for any email address, phone number, or Skype na

9. Here, you will be able to manually remove any suspicious email addresses or phone numbers by clicking the **Remove** button.

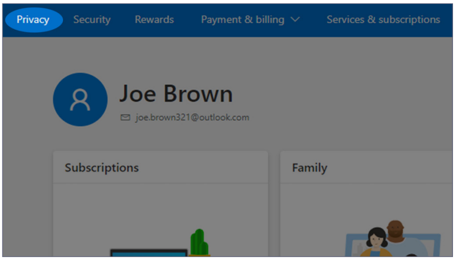
Step 6: Check third party application access

Have you ever linked your Microsoft or Xbox Live account to a third party service? Many websites and applications opt for this method to create a new user account without having to directly request this information from the user. However, the connection this creates between your Microsoft account and the website/application is a common way for hackers to gain access to your email account, without needing your login credentials.

Check if there are any apps or services that have access to your account and remove any that you don't recognise.

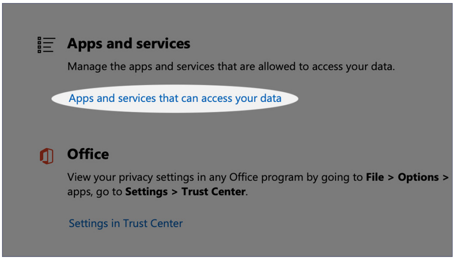


1. Click on your **Profile** icon (top right), click on **My Microsoft Account** or **My Account**.



2. Click on **Privacy** in the top menu bar.

Step 6: Check third party application access CONT...



Apps and services

Manage the apps and services that are allowed to access your data.

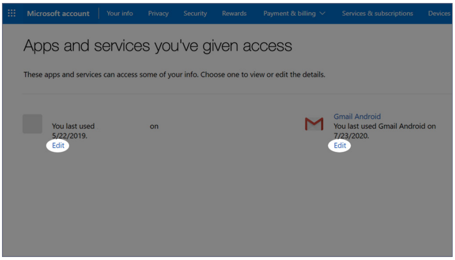
Apps and services that can access your data

Office

View your privacy settings in any Office program by going to **File > Options >** apps, go to **Settings > Trust Center**.

Settings in Trust Center

3. Scroll down to **Other Privacy options** and under **Apps and Services**, click on **Apps and Services that can access your data**.



Apps and services you've given access

These apps and services can access some of your info. Choose one to view or edit the details.

You last used on 5/22/2019.
Edit

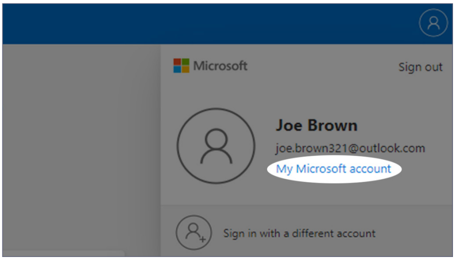
Gmail Android
You last used Gmail Android on 7/23/2020.
Edit

4. This lists all the apps that can access data related to your account.

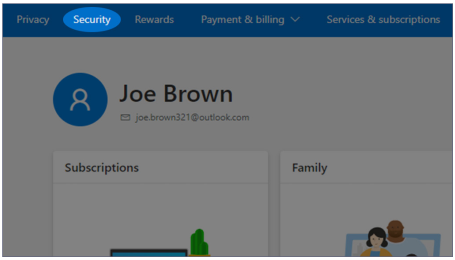
   Click **Edit**, then click **Remove these permissions** for any that you didn't configure yourself.

Step 7: Check login activity

Your login activity is a history of when and where someone has logged into your email account. **Regularly review your login activity to check if your email account has been accessed at unusual times or from unusual locations**.

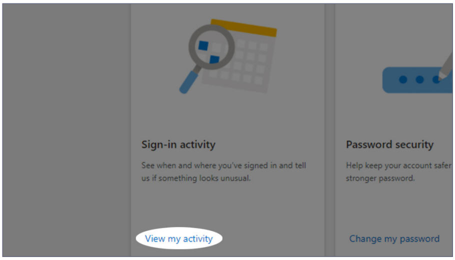


1. Click on your **Profile** icon (top right), click on **My Microsoft Account** or **My Account**.



2. Click on **Security** in the top menu bar. You may have to enter your password again to verify you can make changes to sensitive info.

Step 7: Check login activity CONT...



Sign-in activity

See when and where you've signed in and tell us if something looks unusual.

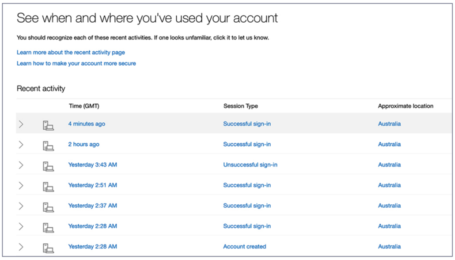
View my activity

Password security

Help keep your account safer stronger password.

Change my password

3. Under Security Basics, on the **Sign-in** activity tile, Click **View my activity**.



See when and where you've used your account

You should recognize each of these recent activities. If one looks unfamiliar, click it to let us know.

Learn more about the recent activity page

Learn how to make your account more secure

Recent activity

Time (GMT)	Session Type	Approximate location
4 minutes ago	Successful sign-in	Australia
2 hours ago	Successful sign-in	Australia
Yesterday 3:43 AM	Unsuccessful sign-in	Australia
Yesterday 2:51 AM	Successful sign-in	Australia
Yesterday 2:37 AM	Successful sign-in	Australia
Yesterday 2:28 AM	Successful sign-in	Australia
Yesterday 2:28 AM	Account created	Australia

4. Here you can check the time and location of the logins into your account to verify that your email account has not been accessed at unusual times or from unusual locations.

   If you see any suspicious activity since your last password change, click on the drop down arrow for that session and click **Secure your account** to change your password. Consider using a unique strong passphrase as your password (see page 7).

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

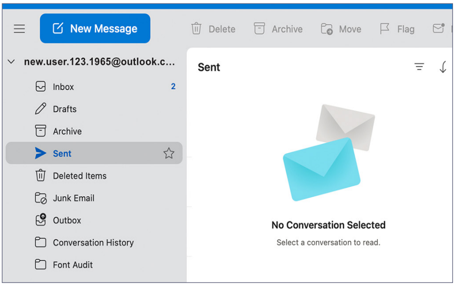
   - The **Device/platform** – is this a device you are familiar with or own?
   - The **Browser/app** – is this something you use?
   - The **Date/Time** – does the login date and time seem out of the ordinary?
   - The **IP address** – was the login from a country you are familiar with?

   Note that if you do go ahead and **Secure your Account**, you will need to verify your identity and change your password. This will also automatically log you out of all other existing sessions.

Step 8: Check your email folders, devices, and other accounts

Check email folders

Once you have made sure only authorised persons have access to your email account, you may want to consider checking your email folders, specifically your sent and deleted items. This will help you assess what actions a cybercriminal has taken if they accessed your account.



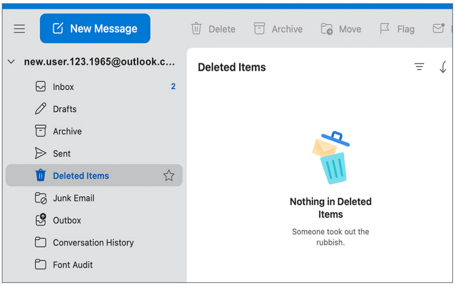
No Conversation Selected

Select a conversation to read.

1. To check sent items, click on **Sent items** in the side menu.

   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. **Check login activity (page 20)** every time you become aware that a criminal contacted someone from your email account.



Nothing in Deleted Items

Someone took out the rubbish.

2. To check deleted items, click on **Deleted items** in the side menu. You can recover deleted items by clicking on **Recover items deleted from this folder**.

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

Run a malware scan

Malware is any software that is specifically designed to disrupt, damage or gain unauthorised access to a device. Use a malware scanning tool to find and remove any malware detected.

1. Do this using the malware scanning tool on your device. You may already have a malware scanning tool that came with your device. If you don't know the name of your malware scanning tool, you can search for it.
2. Type the name of the malware scanning tool. Or press the Windows key on your keyboard for Windows 10 and start typing. Suggested search terms: Antivirus, Microsoft Defender.
3. Once you have found your malware scanning tool, follow the instructions to run a scan and delete any malware identified.

While in progress, take notes or photos of any suspicious software applications, files, pop-ups or other key details you encounter.

For more information for Windows 10 users, read the ACSC's Step-by-Step guide *Performing a malware scan using Microsoft Defender Antivirus for Windows 10* available on **cyber.gov.au**.

Check other linked accounts

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 banking and finance, social media, or other accounts.

If you used the same password or passphrase for your email account and any other accounts, these may be no longer secure. Enable multi-factor authentication where possible on these accounts, and consider changing the passwords to unique strong passphrases.

Notes

ACSC Australian **Cyber Security** Centre

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

🌐 cyber.gov.au

☎ call 1300 CYBER1 (1300 292 371)

Australian Government
Australian Signals Directorate