Lawcover®

CYBER SECURITY SNAPSHOT

PROTECT YOUR EMAIL, CHAT APPS, MESSAGING AND SOCIAL MEDIA

Set up multifactor authentication

Backup chats and communications regularly

Train staff to use messaging, chat apps and social media responsibly

Use DMARC, DKIM and SPF to protect your emails.

Block and report unwanted contacts or spam

Send email attachments securely to minimise interception by cybercriminals

Enable full event logging for all email accounts, with a minimum retention period of 1 year

STEP BY STEP

PROTECT YOUR EMAIL

Set Up Multi-Factor Authentication (MFA)

An extra layer of protection; like having a second lock on your door.

Enable multi-factor authentication (MFA) on your accounts to protect them from cybercriminals who manage to access your passwords fraudulently.

EMAIL

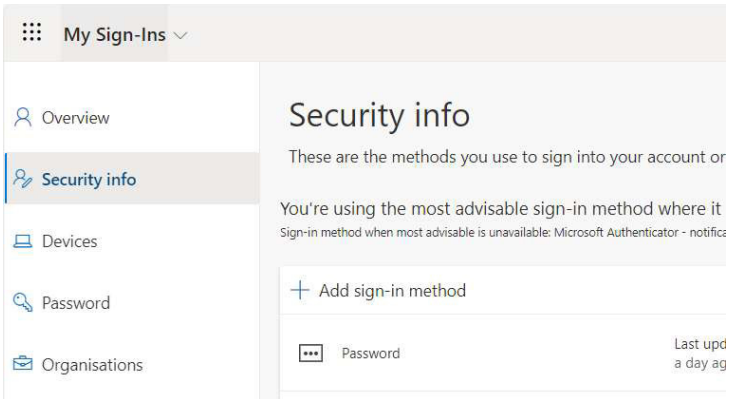
Microsoft

1. Sign in to your Microsoft account at

https://myaccount.microsoft.com/

2. Scroll down to Security info and select
3. Select Security Dashboard
4. Click Add a sign-in Method
5. Click Microsoft Authenticator
6. Download and install the Microsoft Authenticator app
7. Scan the QR code

Once complete you should be asked to sign in with a number that appears on your phone.



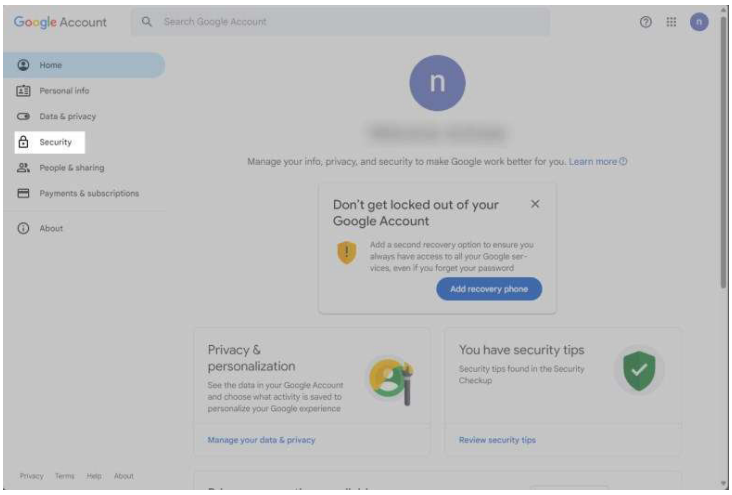
STEP BY STEP
PROTECT YOUR EMAIL
Set Up Multi-Factor Authentication (MFA)

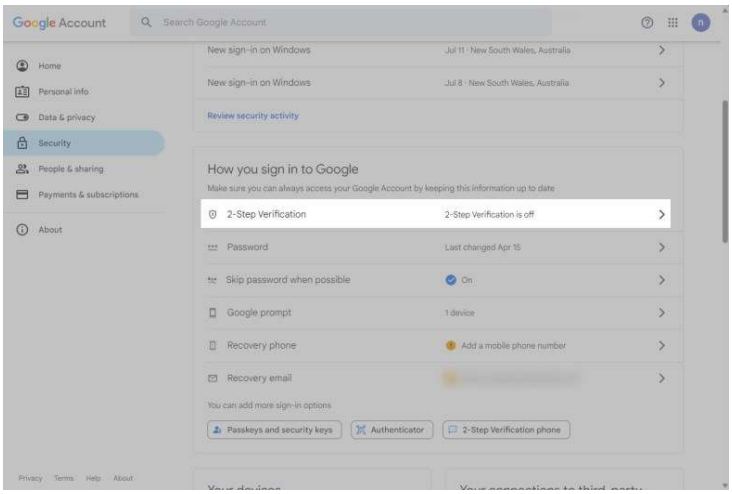
> Multi-factor authentication (MFA) typically requires a combination of something the user knows (pin, secret question), physically possesses (card, token key) or inherently possesses (finger print, retina).

Gmail

1. Sign in to your Google Account
2. On the left navigation panel, click Security
3. On the How you sign in to Google panel, click two-step verification (or MFA)
4. Select Turn on 2-step Verification

Follow the steps on the screen to activate two-step verification (or MFA).





STEP BY STEP

PROTECT YOUR EMAIL

Spam Filtering

Email filtering is the act of processing emails, incoming and sometimes outgoing, to classify and categorise them. This action is usually performed by a mail server is often used to detect spam, viruses, and malware before it reaches the user. Email filters analyse emails for common red flags and if the filter detects those red flags, the email is separated into a spam folder. Common signs of spam emails include:

- Bad IP address
- Poor domain reputation
- Bulk emails
- Suspicious language
- Links in the email body.

Block and Report - emails

Blocking and reporting unwanted contacts or spam protects information and privacy, provides peace of mind and helps authorities identify and disrupt malicious activities.

The specific steps to block and report unwanted contacts or spam vary depending on the email platform you are using however, generally you can:

- Mark as Spam: Flag the email as spam and move it to the spam folder
- Block Sender: Use your email client's settings to block the sender's address.

STEP BY STEP

PROTECT YOUR EMAIL

Data Loss Prevention and Mobile Device Management

Integrating data loss prevention (DLP) and Mobile Device Management (MDM) with email software security controls if highly recommended given the sensitivity of data held by most law practices, as should be imposing restrictions on automatic email forwarding.

Microsoft Purview Message Encryption: What is it?

Microsoft Purview Message Encryption is an advanced email encryption service integrated within the Microsoft 365 suite. Designed to protect sensitive email communications, it ensures that only intended recipients can access the message content. It offers encryption, rights management and secure access controls, even when communicating with external parties, and provides robust confidentiality for client communications. This can help a law practice comply with legal and regulatory requirements for data protection, while enhancing the security of sensitive information shared via email.

**Included in Microsoft 365 E5 Compliance Add-on.*

EMAIL SECURITY

It is recommended that a law practice set up **DMARC**, **DKIM** and **SPF**.

These are email authentication protocols that verify the sender's identity, helping to prevent phishing, spam, and other email-based attacks. These are special DNS settings that your domain account support can help you with. To find out who your domain host is, go to https://who.is and enter your domain in the domain search. This will return the registrar info which can be used to contact and request assistance with setting up these records.

DMARC - Domain-based Message Authentication, Reporting, and Conformance is a tool for enhancing email security and protecting your emails against phishing and spoofing

DKIM - DomainKeys Identified Mail adds another layer by allowing domain owners to digitally sign their outgoing email.

SPF - Sender Policy Framework allows the domain owner to specify which IP address from which email from that domain can be sent.

STEP BY STEP

PROTECT YOUR EMAIL

Secure Email Attachments

Skilled cybercriminals can intercept emails and access attachments along with email content. You can securely share email attachments using Microsoft OneDrive, Dropbox, or Google Drive.

STEP BY STEP

PROTECT YOUR EMAIL

Sending Secure Attachments

Emails are often used to exchange sensitive information, such as financial data, legal contracts, client information and employee information. As a result, mailboxes can become repositories for large amounts of potentially sensitive information and information leakage becomes a serious threat. By 'encrypting' individual email messages (including attachments) containing sensitive or confidential information you ensure that you and your clients stay protected.

Outlook – individual messages

1. Compose a new email: Draft your message as usual
2. Encrypt the message:
   - Click the Options tab
   - Select Encrypt
   - Choose the desired encryption level (e.g., Encrypt-Only, Do Not Forward).
3. Attach your file: Add the file you want to encrypt
4. Send the email: Click Send

Gmail – individual messages

To send attachments securely via Gmail, you can use confidential mode:

1. Compose your email
2. Click Attach
3. Select the files you want to upload
4. Click Turn on confidential mode in the bottom right of the window
5. Set an expiration date and passcode

Mail App on Mac – individual messages

1. Choose File > New Message
2. Move the pointer over the From field
3. Click the pop-up menu that appears
4. Choose the account for which you have a personal certificate in your keychain
5. Address the message to recipients
6. If your keychain contains a personal certificate for every recipient, an encrypted icon (containing a closed lock) is shown

For domain wide encryption of sensitive information, you can use Microsoft Purview.

STEP BY STEP

PROTECT YOUR EMAIL

Turn on Logging

Logging is incredibly important for troubleshooting and diagnosing problems, but more importantly if you experience a breach, the log files will be able to show what happened, when it happened, and how the threat actor gained access to the mailbox.

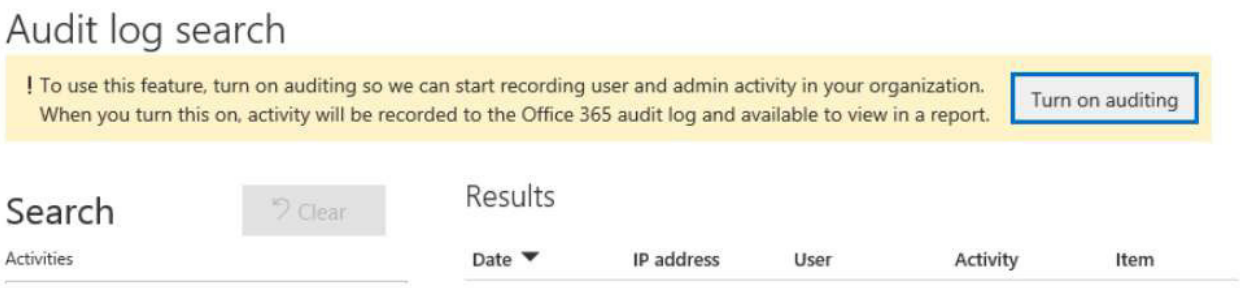
Outlook

1. In Outlook, go to the **File** tab > **Options** > **Advanced**
2. Under **Other**, select or clear the E**nable troubleshooting logging (requires restarting Outlook)** check box
3. Exit and restart Outlook

Office 365

1. Log in to the Security & Compliance Centre of your account here: https://protection.office.com/
2. From the left hand panel click Search > Audit log search
3. If you see “Turn on auditing” on the next screen, click it - see screenshot below

Note: if you don’t see this button, that means auditing is already enabled



STEP BY STEP

PROTECT YOUR CHAT AND MESSAGING APPS

Set up Multi-Factor Authentication (MFA)

An extra layer of protection; like having a second lock on your door.

Enable multi-factor authentication (MFA) on your chat and messaging apps and accounts to protect them from cybercriminals.

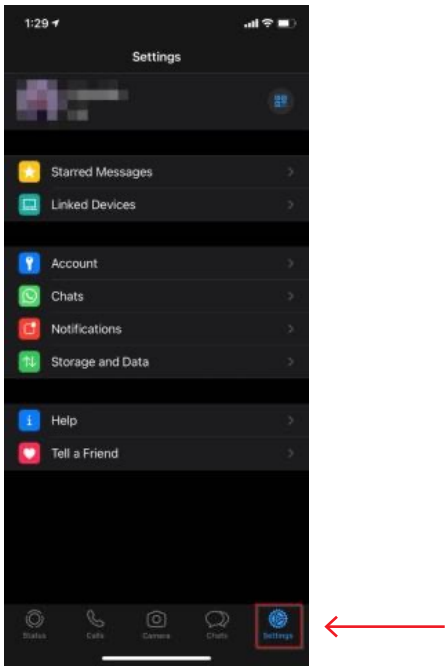
WHATSAPP

How to turn on MFA depends on the software or service you are using. However, the steps are somewhat similar although icons and language may differ slightly depending on the software or device (Android or Apple) you are using.

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.

1 In **WhatsApp** or **WhatsApp Business**, select the **Settings** icon in the bottom right hand corner

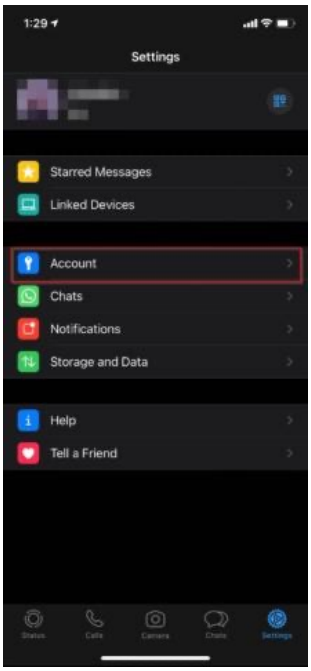
If you use an Android device, you may have to access Settings by tapping three vertical dots in the upper right hand corner of the screen



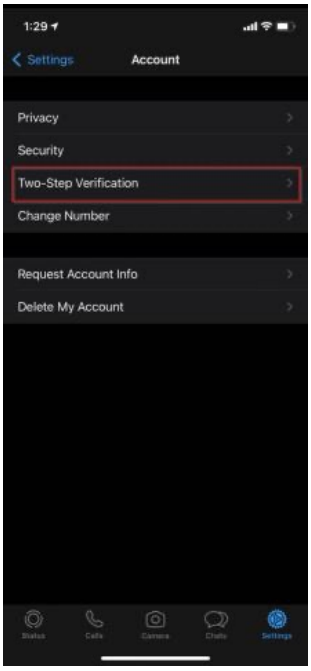
STEP BY STEP
PROTECT YOUR CHAT AND MESSAGING APPS

Set up Multi-Factor Authentication (MFA)

2. Select **Account**



3 Select **Two-Step Verification**

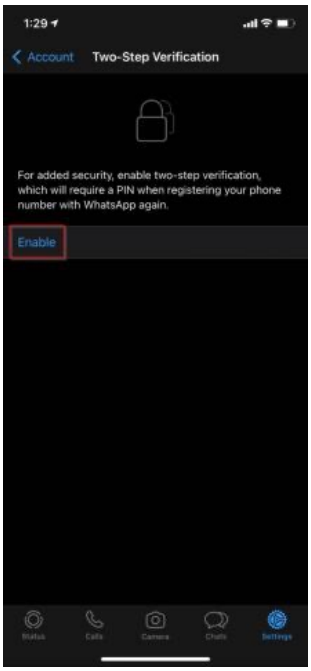


> Messenger services such as WhatsApp, Signal and WeChat are frequently being used by law practices to communicate. This has created a new attack vector for cybercriminals to target individuals with fraudulent messages and to capture important information and communications.

STEP BY STEP
PROTECT YOUR CHAT AND MESSAGING APPS

Set up Multi-Factor Authentication (MFA)

4. Select **Enable**

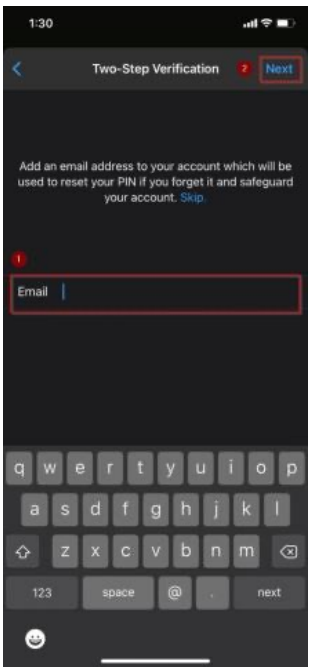


5. Enter a **six-digit PIN**. You will then be asked to confirm your PIN. When complete, select **Next**

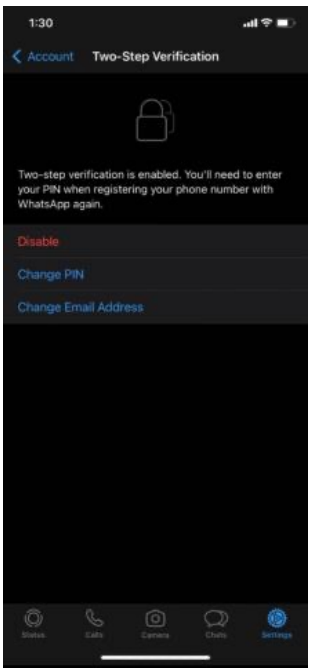
STEP BY STEP
PROTECT YOUR CHAT AND MESSAGING APPS

Set up Multi-Factor Authentication (MFA)

6. Enter your **Email address** and then 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



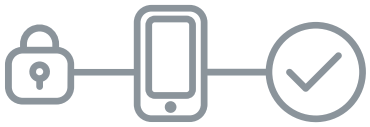
7. After enabling two-step verification you will be returned to this page. The setup is now complete. You can return to this page in the future if you need to change your PIN or recovery email address



Note:

Once MFA is setup, WhatsApp will periodically ask you to enter your PIN.

STEP BY STEP
PROTECT YOUR CHAT AND MESSAGING APPS



Set up Multi-Factor Authentication (MFA)

WECHAT

WeChat does not have an inbuilt MFA feature. However, you can enhance the protection of your WeChat account by taking the following steps:

Common device list

You can set a common devices list for the same WeChat ID to protect your account. By doing this, you can help prevent unknown devices from accessing your account. You can manage your common devices by following the instructions below:

1. **Add device to the list**

   If you've verified your mobile number/email successfully on an infrequently used phone, this phone will be added automatically to your trusted device list

2. **Change the name of device**

   Go to **Me** > **Settings** > **Account Security** > **Manage Devices** > Select one device and tap **Name** in the Details page, then edit the new name and save it

3. **Delete devices from the list**

   You can remove a phone from the trusted device list via **Me** > **Settings** > **Account Security** > **Manage Devices** > **Edit** >Tap the minus symbol before the specific device to delete it

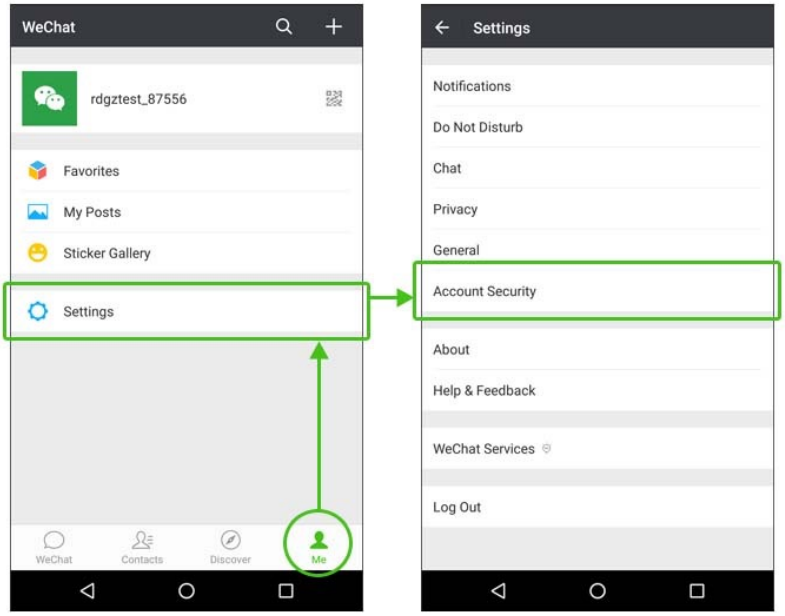
STEP BY STEP
PROTECT YOUR CHAT AND MESSAGING APPS

Set up Multi-Factor Authentication (MFA)

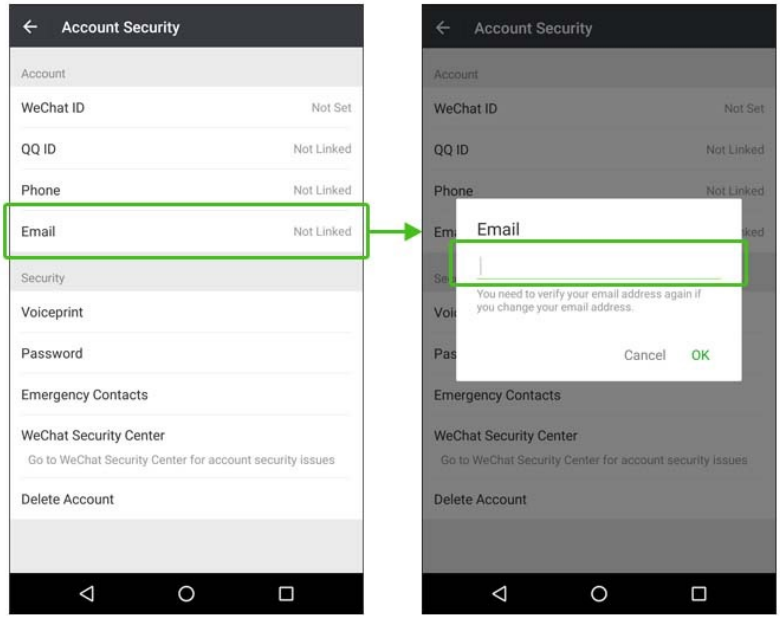
Binding an email address to your WeChat account

Binding an email address to your account will help protect your WeChat account security.

1. From the **Me** tab, choose **Settings**, then **Account Security**



2. More **Settings**, then tap on the **Email field**

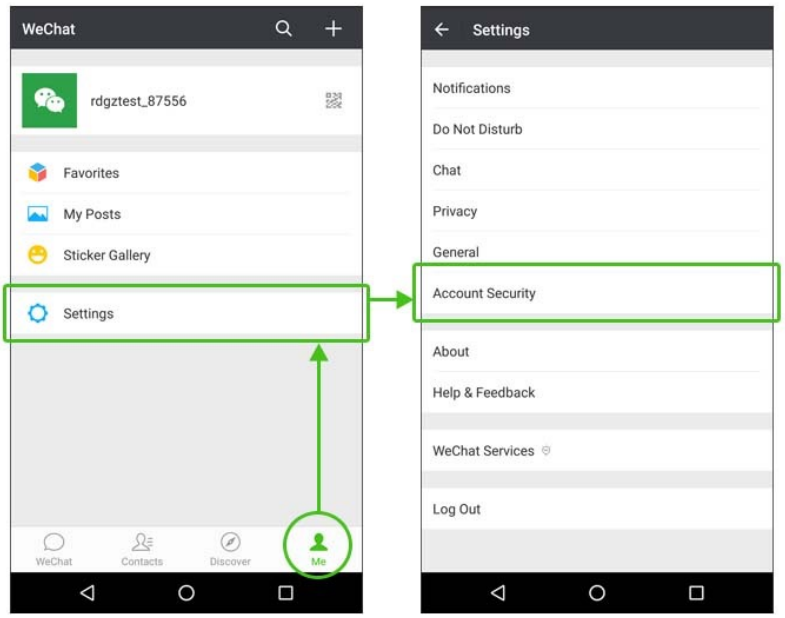


STEP BY STEP
PROTECT YOUR CHAT AND MESSAGING APPS

Set up Multi-Factor Authentication (MFA)

Link your mobile phone number to your WeChat ID.

In WeChat - go to **Me** > **Settings** > **Account Security** the select **Phone**.



You can now retrieve your WeChat password via your linked mobile number giving you an extra layer of protection.

Note:

- You can link your mobile number with only one WeChat ID. You cannot link your phone number with a new WeChat account if you've forgotten your previously linked WeChat ID. In such a case, you can retrieve your password via SMS
- Once you've linked a mobile number on WeChat, you can unlink it only if you link another mobile number
- To help protect your account if you lose your mobile phone or your account is compromised, log in to WeChat from a different device as soon as possible. Then, go to Me > Settings > Account Security > Manage Devices and delete any suspicious devices from the list. For your account's security, you may need to verify your identity when you log in again from any deleted devices.

STEP BY STEP

PROTECT YOUR CHAT AND MESSAGING APPS

Backup and Restore

When using chat apps to communicate it is important that communications are accessible should a cyber breach occur. Backing up your chat data regularly to a secure hard drive or cloud location will protect you and your clients from potential data loss, which may occur from hardware failures, theft, or other cyber-attacks.

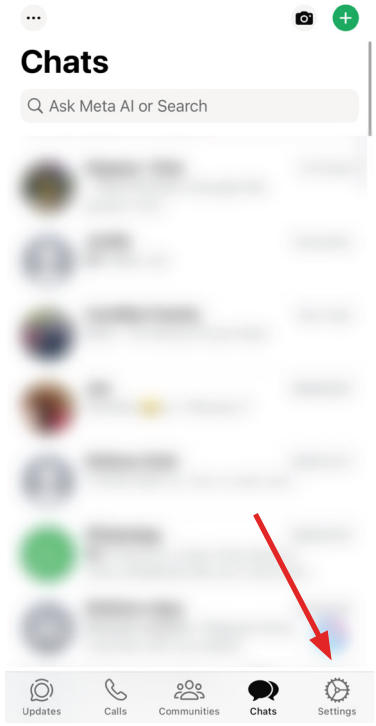
WHATSAPP

Backup

Backup WhatsApp chat history using the built-in feature that lets you save chats to either iCloud (Apple iOS) or Google Drive (Android) respectively.

Apple iOS

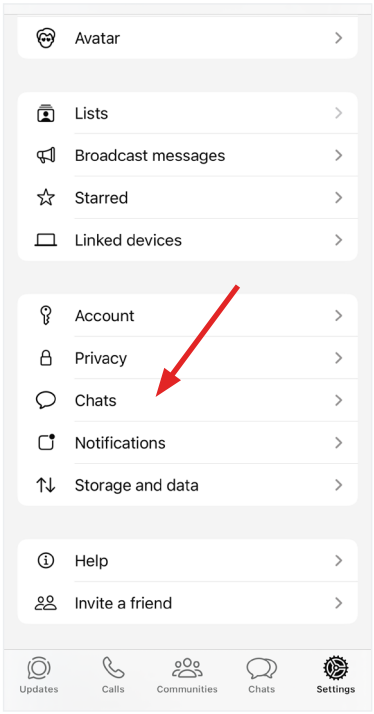
1. When you open WhatsApp from your home screen, you'll notice five buttons along the bottom. Tap the **settings** option on the far right, labelled

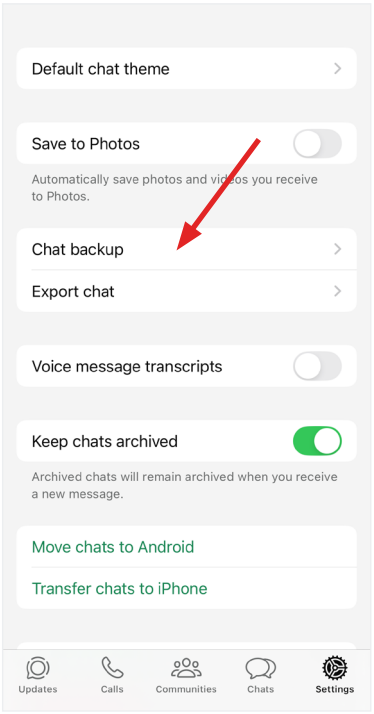


> Regular backups will ensure your chat history and communications can be called upon should the need arise.

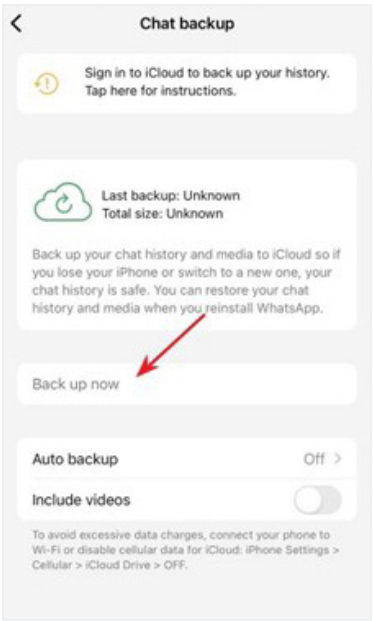
STEP BY STEP
PROTECT YOUR CHAT AND MESSAGING APPS
Backup and Restore

2. In your settings, tap on Chats followed by Chat backup





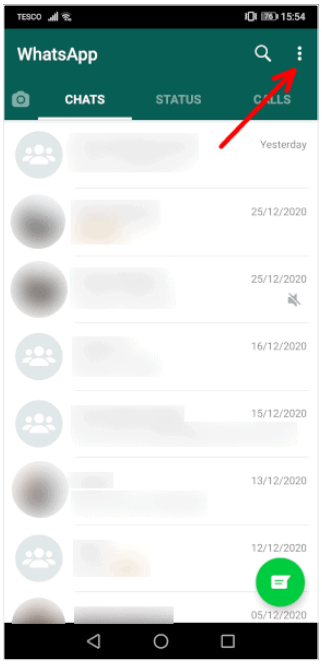
3. You can either tap Back Up Now to start the backup process or select Auto Backup and change/schedule your backup frequency



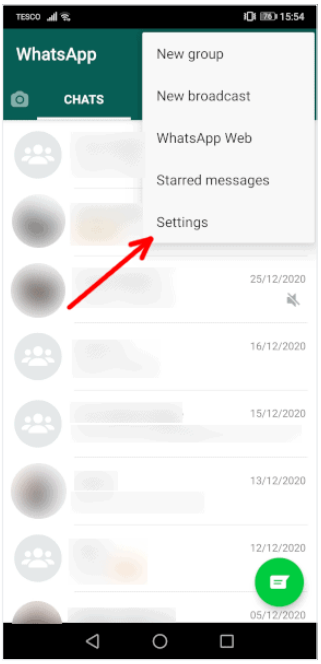
STEP BY STEP
PROTECT YOUR CHAT AND MESSAGING APPS
Backup and Restore

Android

1. Open WhatsApp on your phone and select the menu icon — the **three vertical dots** in the top-right corner



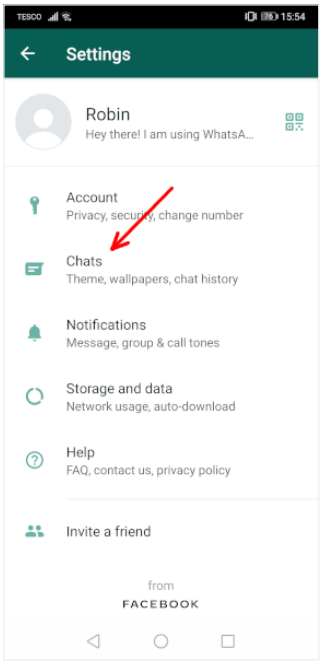
2. Choose Settings from the dropdown list



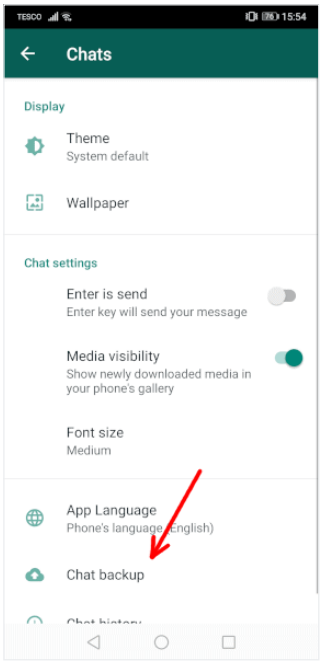
> Ensure that an offline backup is kept separate from your network or in a cloud service designed for this purpose.

STEP BY STEP
PROTECT YOUR CHAT AND MESSAGING APPS
Backup and Restore

3. In WhatsApp's settings, tap Chats to get access to your conversation settings

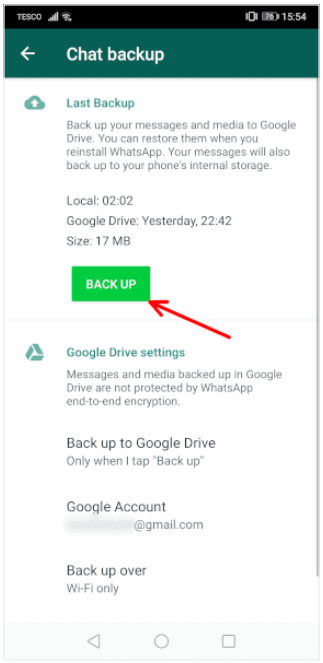


4. Select Chat Backup near the bottom of the page, next to an icon in the shape of a cloud



STEP BY STEP
PROTECT YOUR CHAT AND MESSAGING APPS
Backup and Restore

5. Tap Backup to do a manual backup or Backup to Google Drive to set your backup frequency. If you haven't connected your phone to a Google account, it will only create a local backup



Restore

Apple iOS and Android

When you install WhatsApp on your phone, it will ask you if it should restore chat histories. Make sure that your backup is connected to your cloud storage — either Google Drive or iCloud — before downloading it, and then choose that option when it appears.

> Backups should be tested periodically to ensure their integrity. This can be done by using the restore method.

STEP BY STEP
PROTECT YOUR CHAT AND MESSAGING APPS
Backup and Restore

WECHAT

Backup your WeChat chat history on your phone to your computer via WeChat for Windows/Mac and restore your phone's chat history from your computer backups.

The feature requires installing WeChat for Windows/Mac on your computer. Download and install WeChat for Windows/Mac at https://www.wechat.com/

Backup

- Connect your mobile and computer to the same Wi-Fi network
- On WeChat for Windows/Mac, tap the icon in the lower-left corner > Backup and Restore. Then, on your mobile, select the chat history you want to backup
- Confirm to begin backing up. Don't disconnect from the network or close WeChat until the backup is completed.

Restore

- Connect your mobile and computer to the same Wi-Fi network
- On WeChat for Windows/Mac, tap the icon in the lower-left corner > Backup and Restore > Restore on phone Select the chat history you want to restore
- Tap Confirm on your mobile to begin to restore the chat history. Don't disconnect from the network or close WeChat until the chat history has been restored.

Note:

- Connect your mobile phone and computer to the same network before backing up chat history
- Multiple chat history backups can be saved to the computer. Unwanted chat history backups can be deleted
- When restoring a chat history to your mobile, the backed up version of the chat history will be merged with the chat history already on the mobile. The chat history on the mobile will not be deleted
- WeChat for Android 6.3.31 or higher must be installed on the mobile.

STEP BY STEP

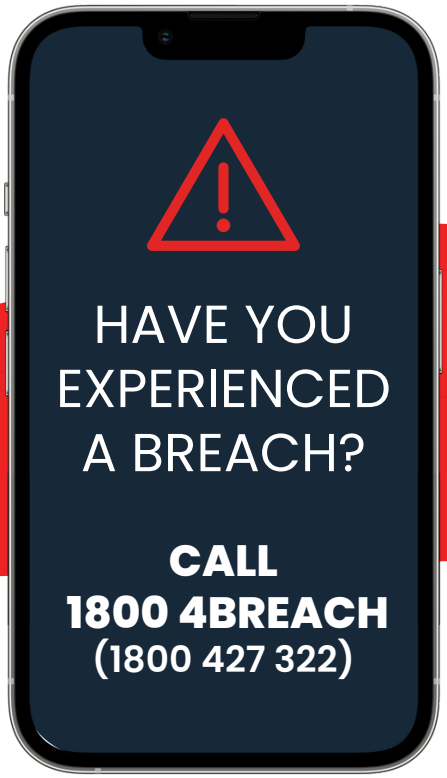
PROTECT YOUR SOCIAL MEDIA

General Security

There are many social media platforms that are used on both a professional and personal level. Popular ones include ‘X’ (formally Twitter), Instagram, Facebook, LinkedIn and YouTube. Exercise caution when using any social media platform, put security measures in place to safeguard against attack and manage each account carefully.

- Keep track of your accounts
- Use multi-factor authentication or random passwords to secure your accounts
- Do not share your passwords or passphrases with anyone
- Set up security questions to recover social media accounts, don’t use questions/answers which are easily guessable
- Do not configure social media accounts to automatically sign in from shared devices such as those used in the office/internet cafes
- Remember to sign out of social media accounts after use on shared devices
- Deactivate your old social media accounts when they are no longer required
- Use the platform’s blocking feature to prevent interactions with unwanted users
- Report spam to the platform’s support team.

Refer to the individual application to configure security recommendations.



Lawcover®

Lawcover Insurance Pty Ltd | ABN 15 095 082 509
Phone (02) 9286 8877 | practicesupportservices@lawcover.com.au | lawcover.com.au