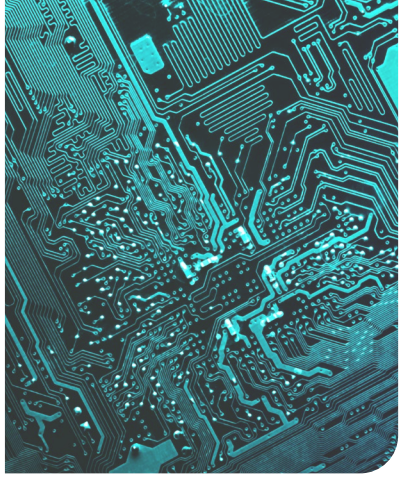
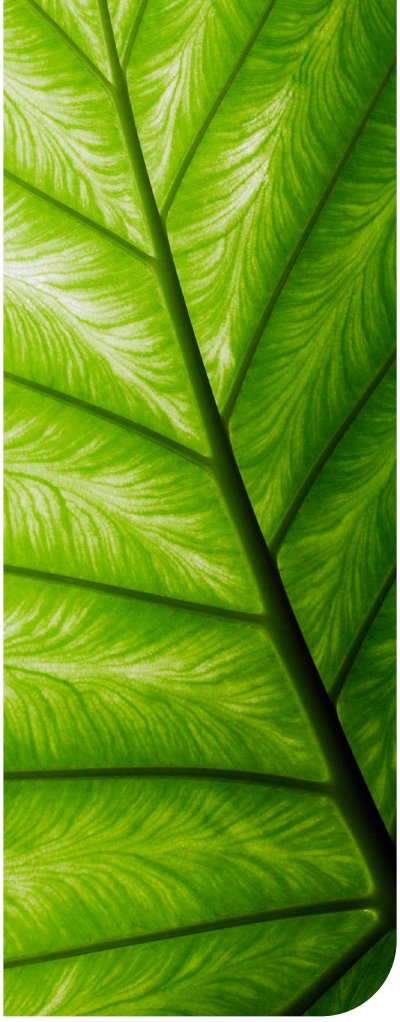
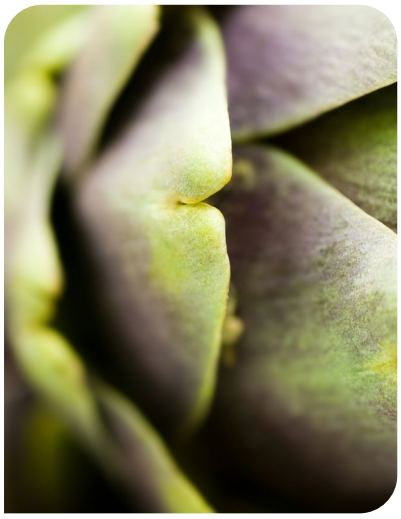



Best security practices

Messaging & social media platforms

RelianceCyber

THOUGHT LEADERSHIP E-BOOK SERIES

General advice

Ensuring the security of your social media accounts is crucial. Here are some general tips that apply to most platforms:

1. Strong and Unique Passwords:

- Use unique passwords for each social media account.
- Create strong passwords with a mix of uppercase and lowercase letters, numbers, and special characters.
- Avoid using easily guessable information like birthdays or common words.

2. Two-Factor Authentication (2FA):

- Enable 2FA whenever possible. It adds an extra layer of security by requiring a second verification method (such as a text message or authentication app) in addition to your password.

3. Beware of Phishing:

- Be cautious of suspicious emails, messages, or links. Scammers often impersonate social media platforms to steal login credentials.
- Verify the legitimacy of any requests for personal information.

4. Privacy Settings:

- Regularly review and adjust your privacy settings. Limit who can see your posts, friends list, and personal details.
- Be mindful of what you share publicly.

5. App Permissions:

- Be selective when granting permissions to third-party apps. Only allow access to necessary information.
- Periodically review and revoke access for apps you no longer use.

6. Regularly Update Apps and Devices:

- Keep your social media apps and devices up to date. Updates often include security patches.
- Use official app stores to download apps.

7. Secure Your Email Account:

- Your email account is often linked to social media accounts. Ensure its security with a strong password and 2FA.

8. Log Out from Shared Devices:

- Always log out from public or shared computers or devices.
- Clear browser cache and cookies after use.

9. Monitor Account Activity:

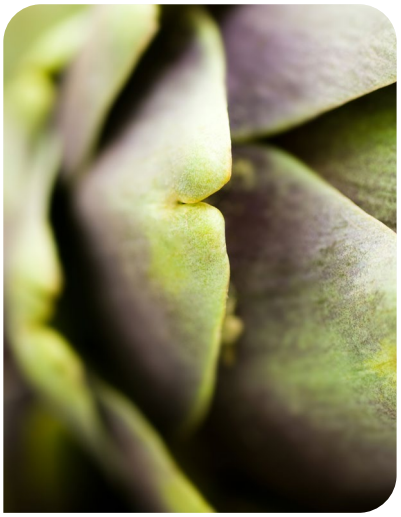
- Regularly check your account activity for any unauthorised logins or suspicious actions.
- Set up alerts for unusual activity.

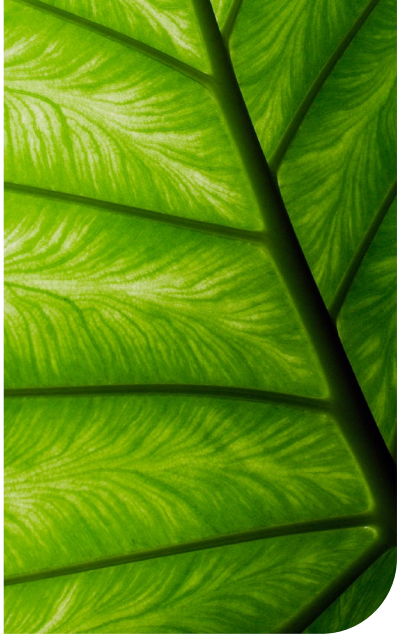
10. Educate Yourself:

- Stay informed about common social media scams and security threats.
- Read official security guidelines provided by the platform.

Proactive measures can significantly reduce the risk of unauthorised access and protect your personal information.

CONTENTS



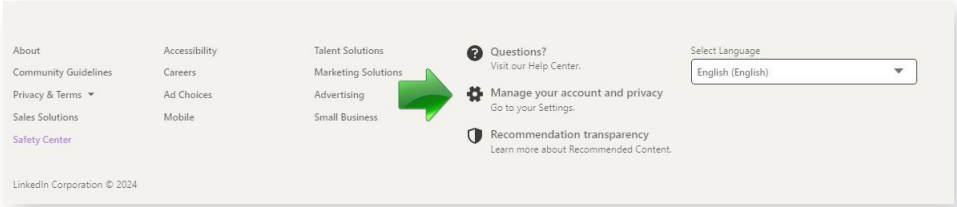


Best Security Practices:

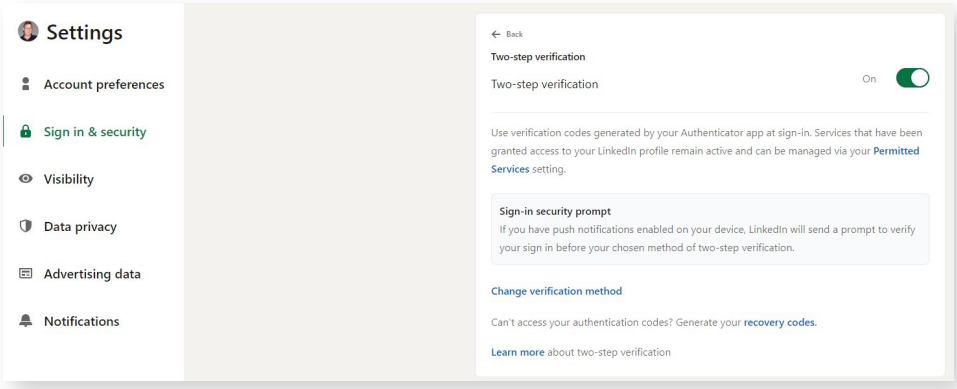
Messaging & social media platforms

LinkedIn security guide

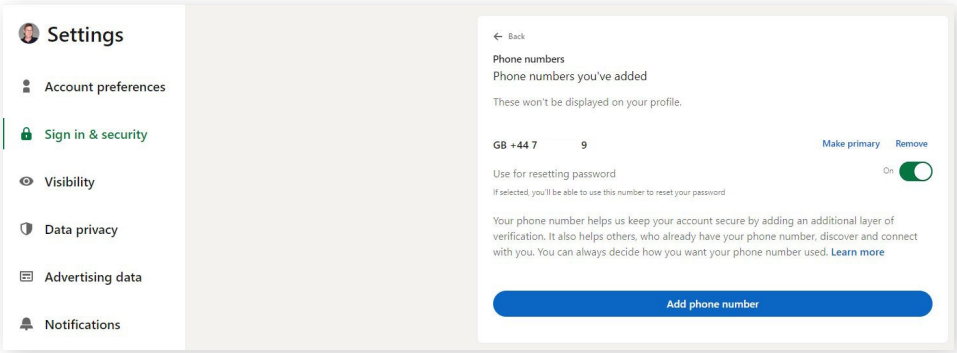
https://www.linkedin.com/help/linkedin/answer/a1375084
The LinkedIn settings option is found at the bottom of the page



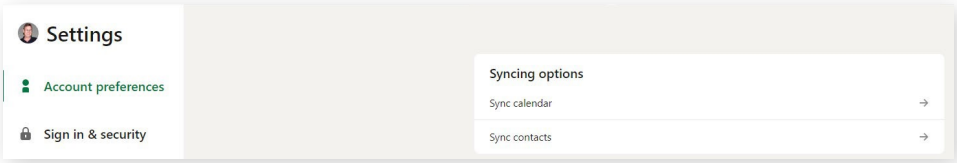
Enable 2-factor authentication (2FA)



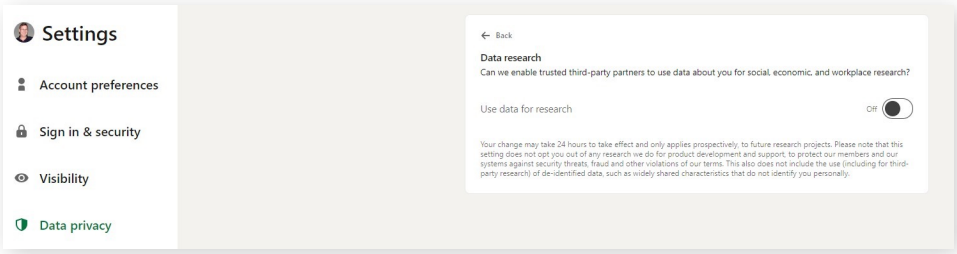
Add a phone number



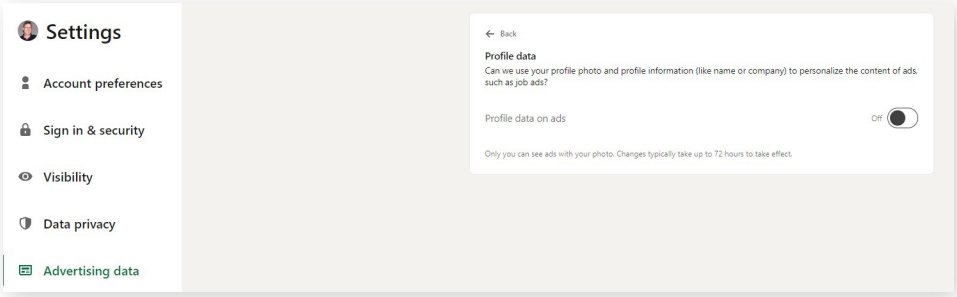
Don't Sync your contacts and calendar



Don't share your data with researchers

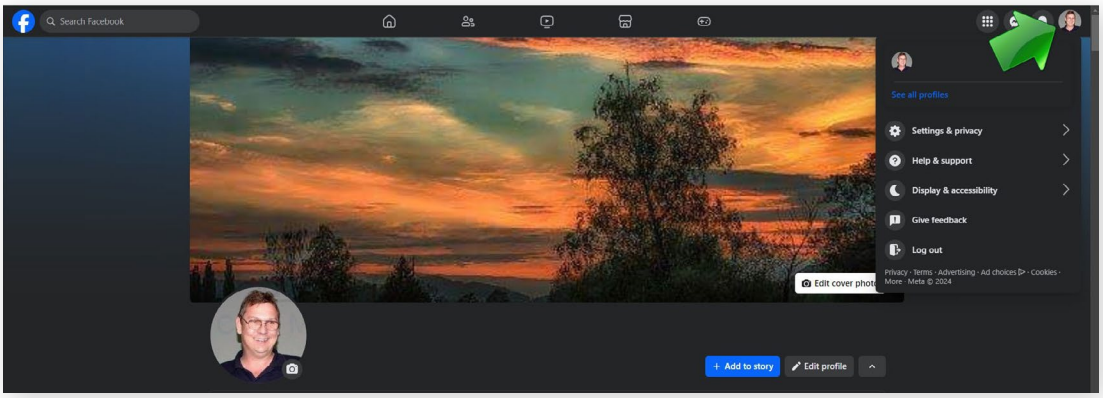


Don't share your data with advertisers

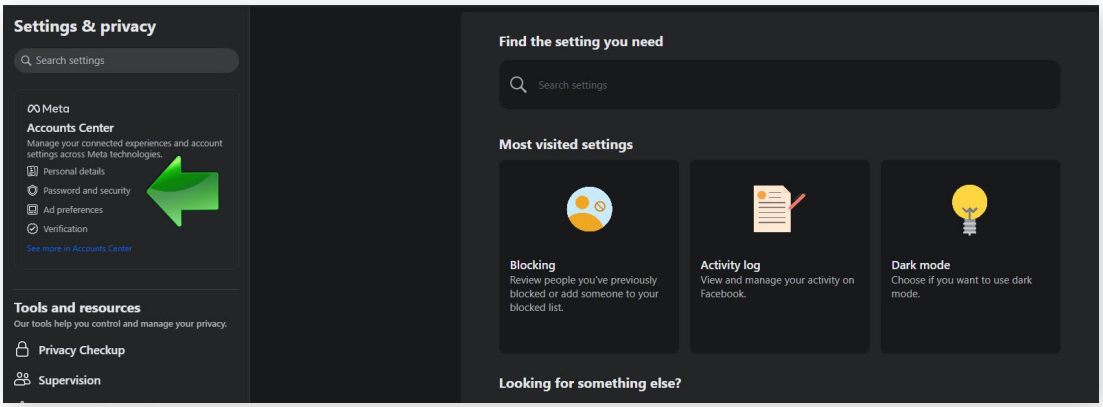


Facebook security guide

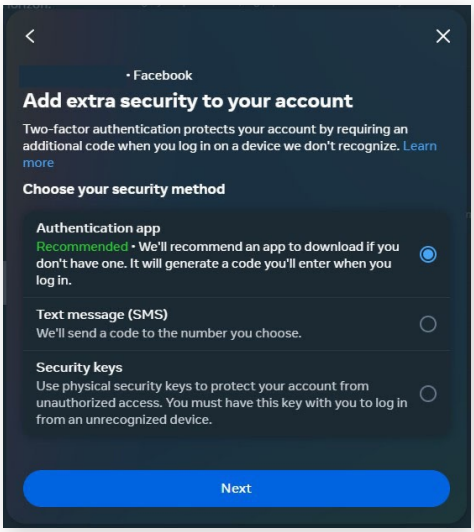
Select ‘Settings and Privacy’



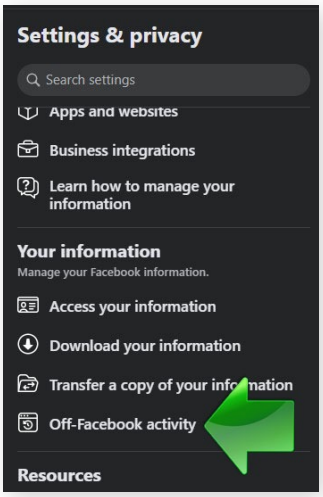
Select ‘Password and Security’



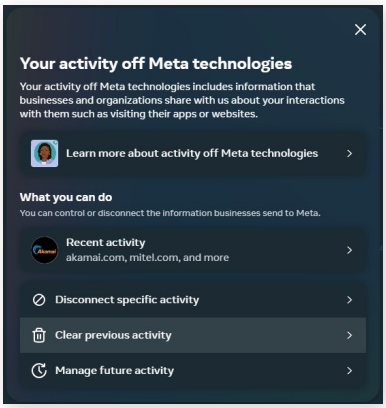
Select ‘Add Extra Security to Your Account’ and select how you want to authenticate

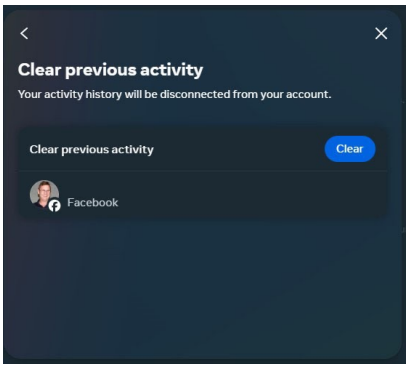


Go back to the settings and privacy menu and select ‘Off-Facebook Activity’

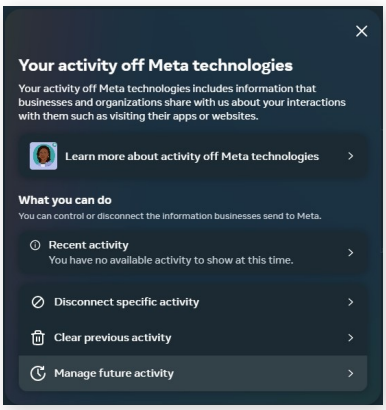


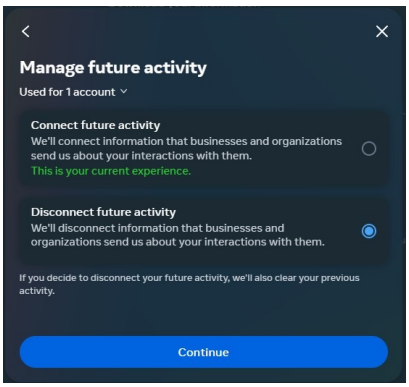
Select ‘Clear Previous Activity’ and then click the ‘Clear’ button



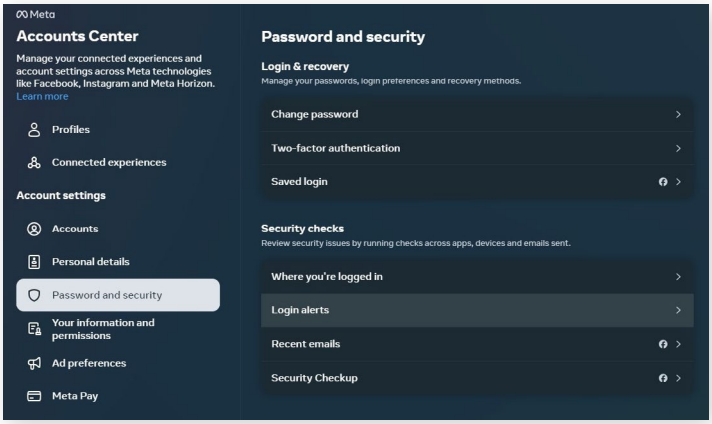


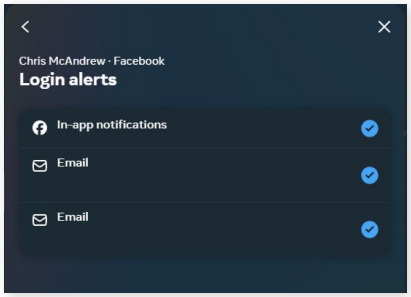
Select ‘Manage Future Activity’ and then select ‘Disconnect Future Activity’



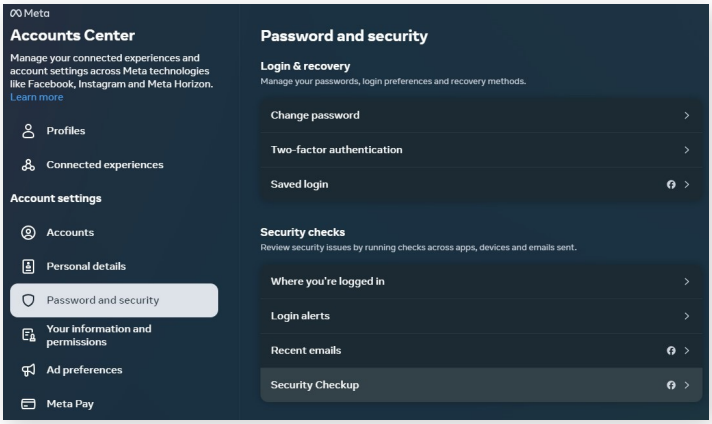


Go back to the menu and select ‘Login Alerts’ then select how you wish to be notified





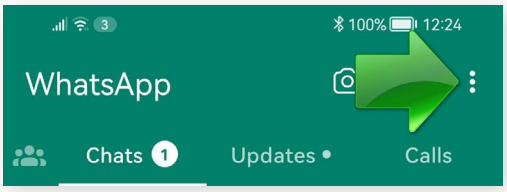
Return to the menu and select ‘Security Checkup’



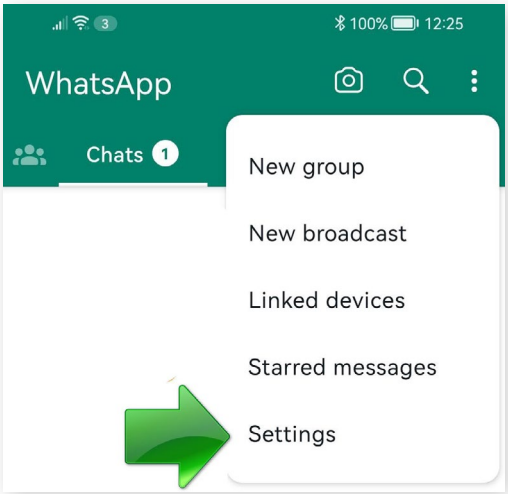
Follow the prompts and adjust as required

WhatsApp security guide

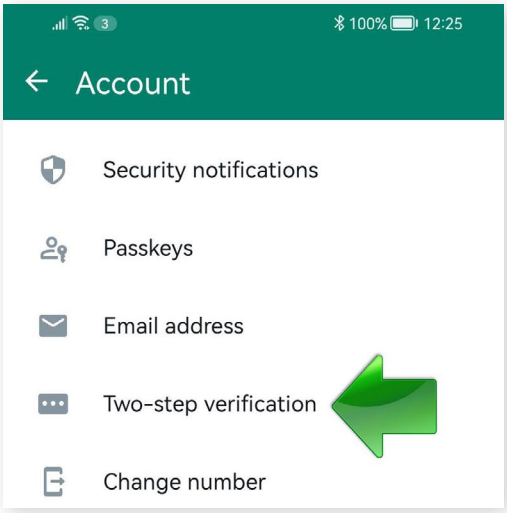
Enable two-step verification by first tapping on the menu



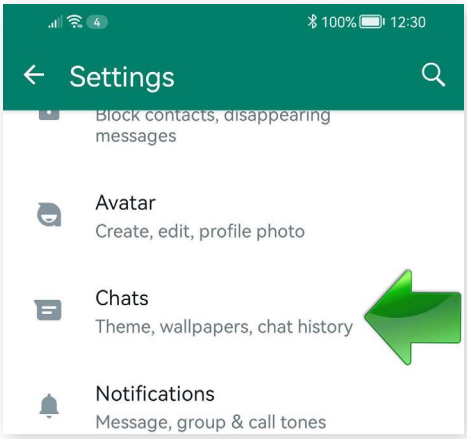
Select 'Settings'



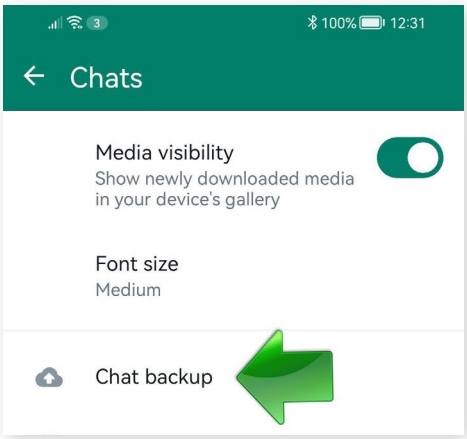
Select 'Two-Step Verification' and follow the prompts



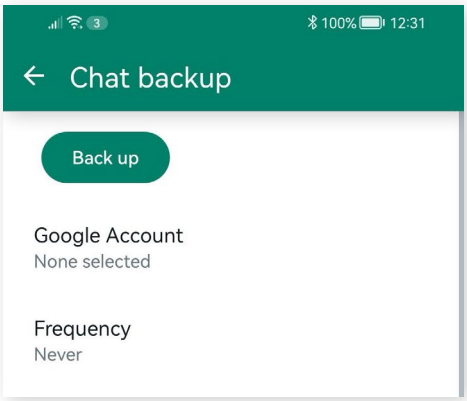
To disable automatic cloud backups, in the settings menu tap ‘Chats’



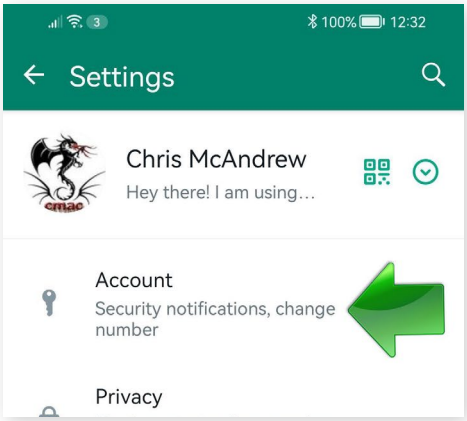
Then tap ‘Chat Backup’

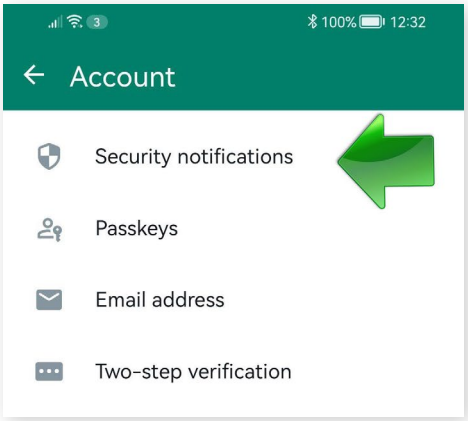


Tap on ‘Frequency’ and select ‘Never’

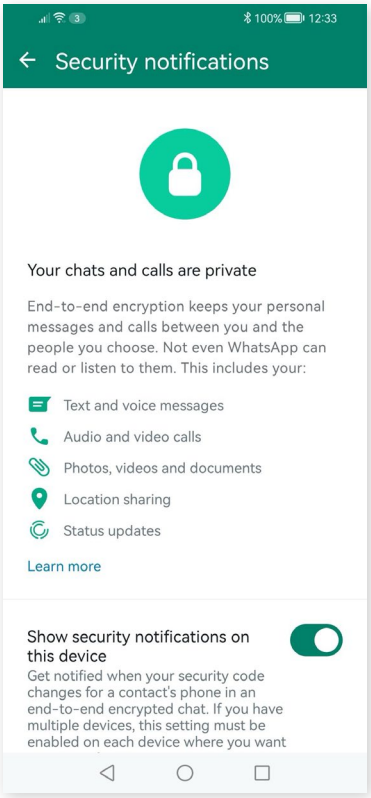


To turn on security notifications tap on ‘Account, then tap ‘Security notifications’





Tap ‘Show security notifications on this device’



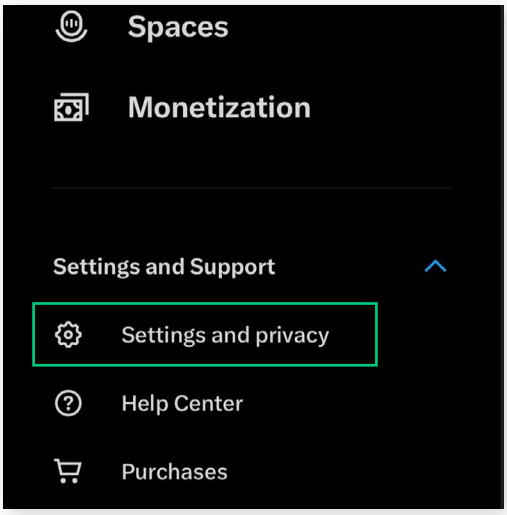
X (Twitter) security guide

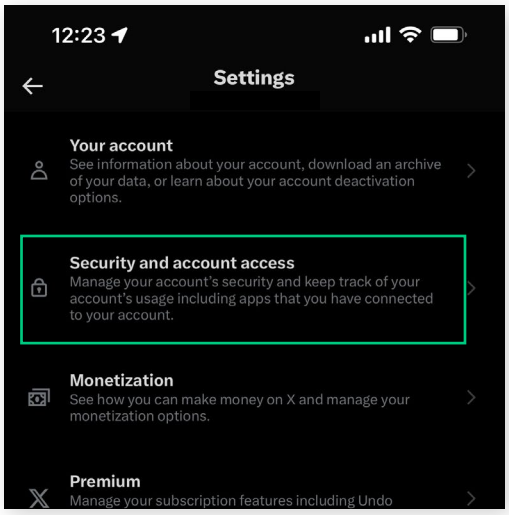
To help keep your account secure, we recommend the following best practices:

- Use a strong password that you don't reuse on other websites.
- Use **two-factor authentication**.
- Require **email** and **phone** number to request a reset password link or code.
- Be cautious of suspicious links and always make sure you're on twitter.com before you enter your login information.
- Never give your username and password out to third parties, especially those promising to get you followers, make you money, or verify you.
- Make sure your computer software, including your browser, is up-to-date with the most recent upgrades and anti-virus software.
- Check to see **if your account has been compromised**.

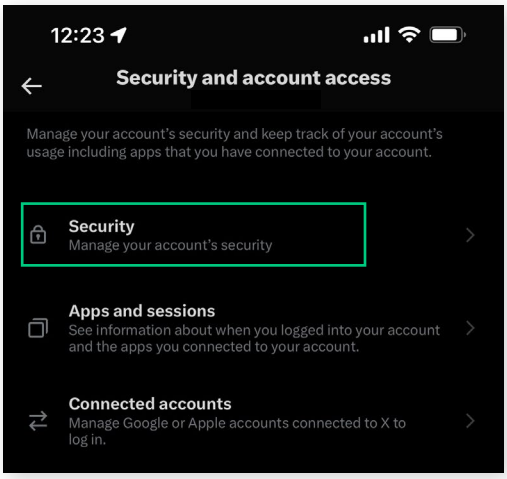
See the full guide here : **https://help.twitter.com/en/safety-and-security/account-security-tips**

To setup Two factor authentication tap your user image in the top-left, then tap 'Settings and privacy', then 'Security and account access'

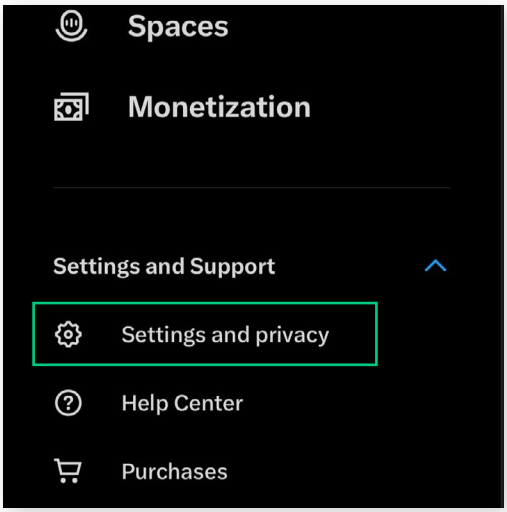


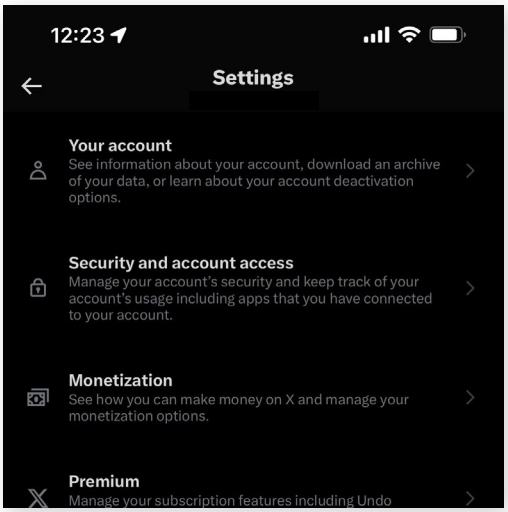


Tap 'Security' and then 'Two-factor authentication'. You can then setup how you want to receive an authentication code.

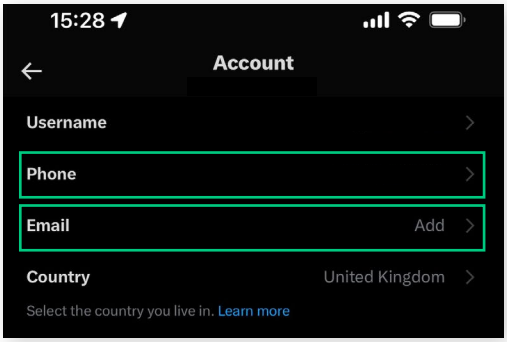


To activate the feature where you require additional information to reset the account password, tap your user image in the top-left, then tap 'Settings and privacy', then 'Your account'

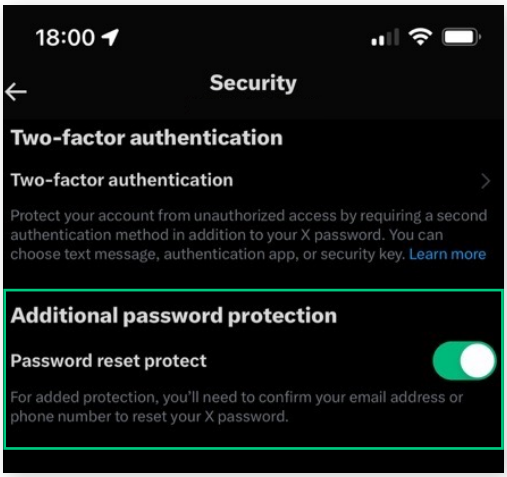




Ensure you have added a phone number and email address



Then in the Security section of your account settings ensure 'Password reset protect' is activated



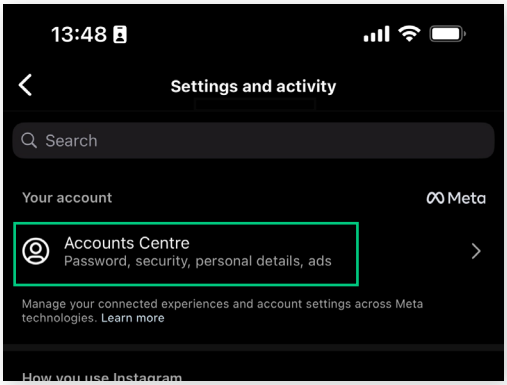
Instagram security guide

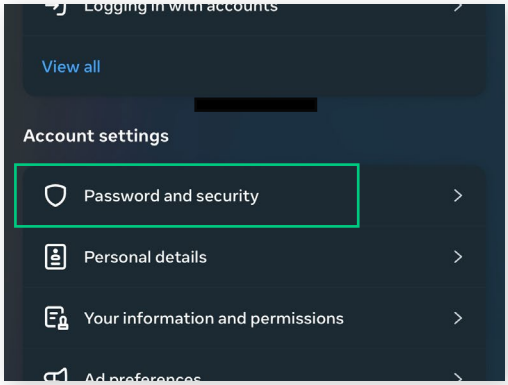
There are several things you can do to help keep your account safe:

- Turn on **two-factor authentication** for additional account security.
- Think before you **authorize any third-party app**, you should never share your login information with an app you don't trust. If you give these apps your login information, whether with an access token or by giving them your username and password, they can gain complete access to your account.
- Pick a strong and unique password that you haven't used for other accounts. Use a combination of at least six numbers, letters and special characters (like !$@%), and try to avoid repetition.
- Change your password regularly, especially if you see a message from Instagram asking you to do so. During automated security checks, Instagram sometimes recovers login information that was stolen from other sites. I**f Instagram detects that your password may have been stolen**, changing your password on Instagram and other sites helps to keep your account secure and prevent you from being hacked in the future.
- **Download your data**. You can keep a backup of your data by requesting a copy of everything you've shared on Instagram in a machine readable HTML or JSON format. Note: You'll need your Instagram account password to request this information.
- Log out of Instagram when you use a computer or phone you share with other people. Don't check the "Remember me" box when logging in from a public computer, as this will keep you logged in even after you close the browser window.

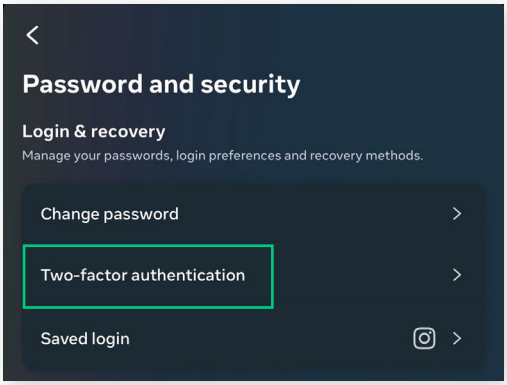
See the full guide here : **https://help.instagram.com/566810106808145?helpref=faq_content**

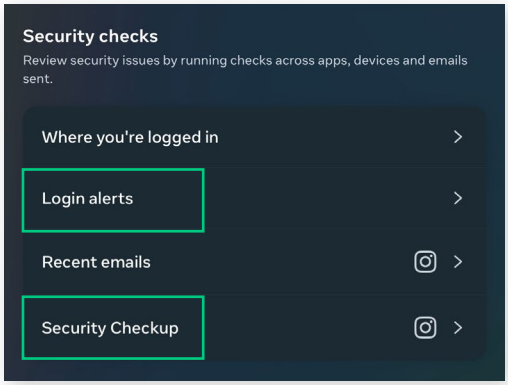
Tap the user icon in the bottom menu, then 'Settings and activity', then 'Accounts centre' and then 'Password and security'.



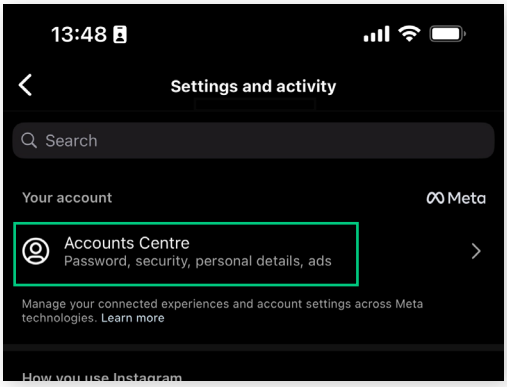


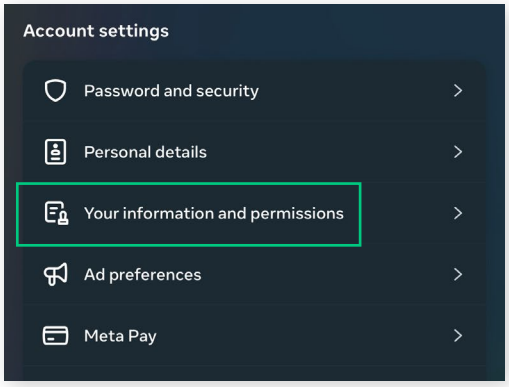
Within the 'Password and security' menu you can setup 'Two-factor authentication', 'Login alerts' and run a 'Security checkup'.



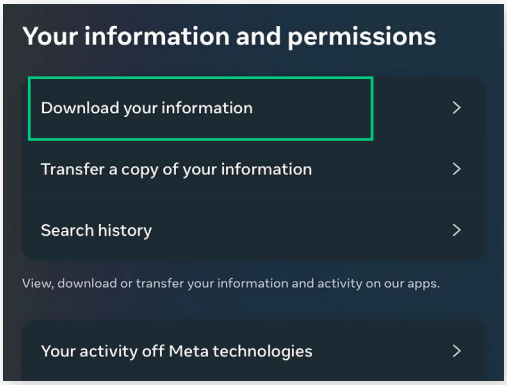


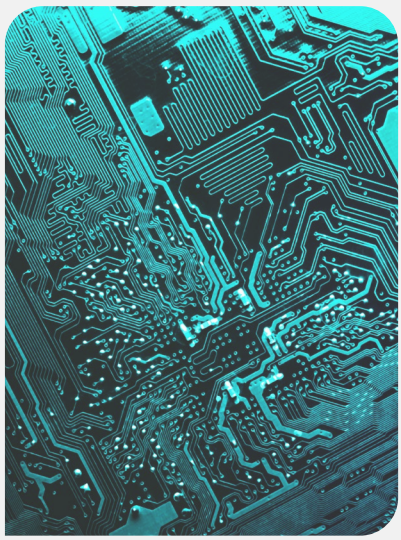
To download all your information from Instagram, tap the user icon in the bottom menu, then 'Settings and activity', then 'Accounts centre' and then 'Your information and permissions'.

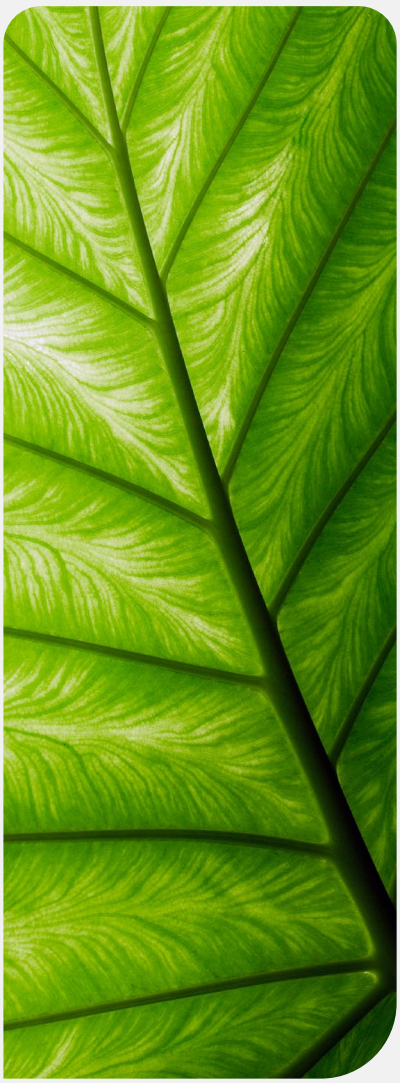


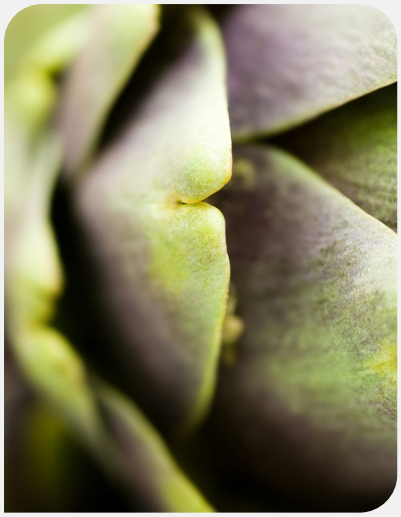


Then tap 'Download your information'









Best security practices

Explore the leadership series

RelianceCyber

reliancecyber.com