Cyber Awareness

How to Manage Social Media Privacy & Security Settings

Are you aware of who can see the information you share online?

Learn how to view and manage your Privacy and Security Settings.

Devon & Cornwall POLICE

January 2025

Contents

Foreword

Welcome to your guide on managing privacy and security in the digital age.

Social media platforms have revolutionised how we connect, share, and engage with the world.

This booklet covers essential privacy and security tips for some of the most popular social media platforms: Facebook, Instagram, X (formerly Twitter), WhatsApp, Snapchat, TikTok, YouTube (Google), and LinkedIn. Each section will provide you with the knowledge and tools you need to take control of your online presence and protect your personal information.

In the following pages, you'll learn how to customise your privacy settings, secure your accounts, and navigate the features and controls that each platform offers.

By taking proactive steps, you can enjoy the benefits of social media while ensuring your information remains safe and private.

Devon and Cornwall Police
Cyber Protect
Digital Capabilities Unit
Email : cyberprotect@dc.police.uk

The Importance of Strong & Complex Passwords

Your smartphones, tablets, and computers hold a lot of important personal information, such as photos, messages, and details of your online accounts. It's essential to keep this information safe from anyone who shouldn't have access. Using passwords is a simple and effective way to protect your devices and the data stored on them.

When used correctly, passwords help ensure that only you can access your information, keeping it secure and private.

Tip 1:

Create strong passwords

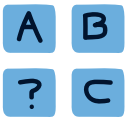
Use long passwords that include a mix of upper- and lower-case letters, numbers, and special characters. Aim for a password that is 12-16 characters long, as longer passwords are generally more secure. Avoid using easily guessed information like pets' names, birthdays, or common words. Instead, consider using a passphrase made up of three random words to create a strong and memorable password.

If you find it difficult to remember your passwords, you can use a password manager to securely store them.

Tip 2

Don't use the same password everywhere

It's important to have a unique password for each of your accounts. If someone gains access to one password, they could potentially use it to access your other accounts as well. By creating different passwords, you help ensure that if one account is compromised, your other personal information remains safe. This practice adds an extra layer of security, protecting your sensitive data from unauthorised access.



Tip 3

Use three random words

A good way to make your password difficult to crack is by combining three random words to create a password (for example applenemohotel). Or you could use a password manager, which can create strong passwords for you (and remember them).

The Importance of Two-Step Verification (2SV)

Two-Step Verification, or Two-Factor Authentication, is an important security feature that adds an extra layer of protection to your online accounts. By requiring two forms of verification before allowing access, 2SV helps keep your personal information safe, even if someone gets hold of your password. Understanding how 2SV works and how to set it up can greatly enhance your online security.

How does Two-Step Verification work?

When you enable 2SV on an account, you'll need to provide two types of information to log in:

1. **Something You Know**: This is usually your password.
2. **Something You Have**: This could be a code sent to your mobile phone, a code generated by an authentication app, or even a physical security key.

This means that even if someone else knows your password, they still cannot access your account without the second form of verification.

Ensure that the phone number or email address associated with your account is current. If you need to recover access, having up-to-date information is crucial.

Tip 1:
Enable 2SV on all important accounts

Turn on 2SV for your email, banking, and any other accounts that hold sensitive information. This adds an extra layer of security to your most valuable accounts.

Tip 2:
Choose an authentication method that works for you

When setting up 2SV, you'll usually have a few options for how to receive your verification codes. You can choose to get codes via text message, an email, or an authentication app. Pick the method that you find easiest to use and remember.

Tip 3:
Beware of phishing/scam attempts

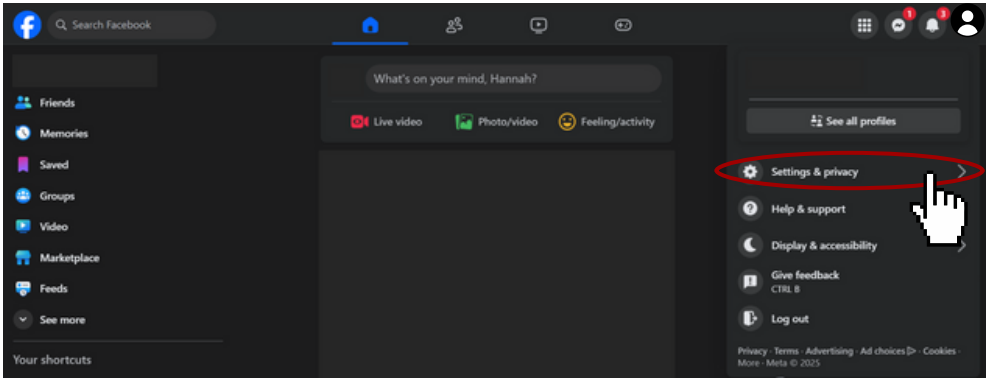
Be aware of emails or messages that ask for your 2SV codes. Legitimate companies will never ask for this information directly. If you receive such a request, do not respond, and report it instead.

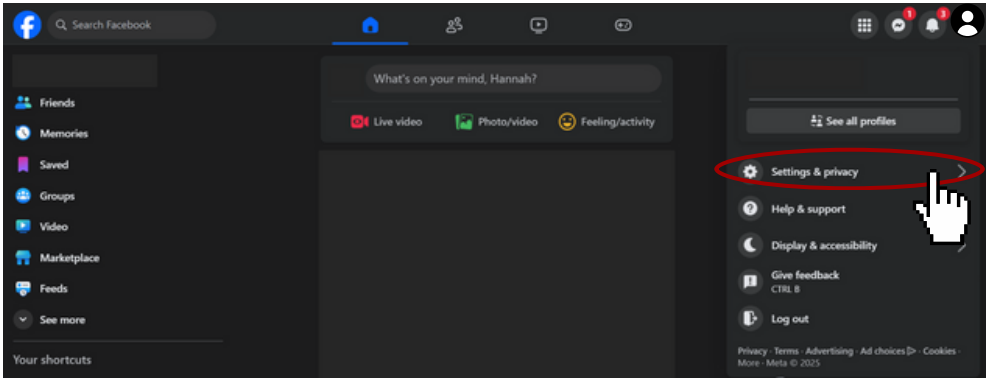
Facebook (Meta)

Facebook, owned by Meta, offers a Privacy Check-up tool. This feature provides a quick and easy way to review and manage your privacy settings.

By using the Privacy Check-up, you can ensure that your information is only shared with the people you want, enhancing your online security and peace of mind. This tool simplifies the process of customising your privacy preferences, making it accessible for all users to take control of their digital presence.

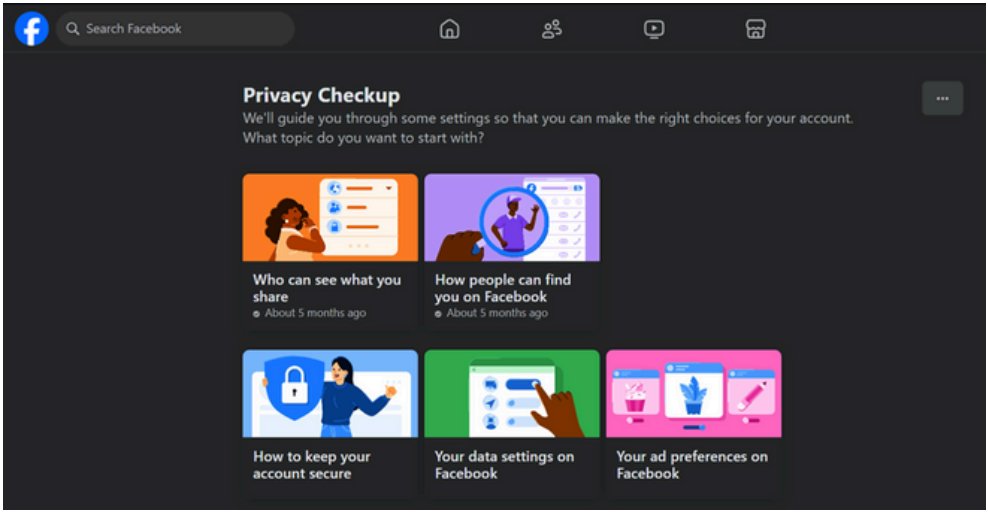
The Privacy Check-up tool can be accessed on Facebook by clicking your profile icon in the top right corner, then selecting 'Settings & Privacy' from the drop-down menu. From here you can select 'Privacy Checkup'.



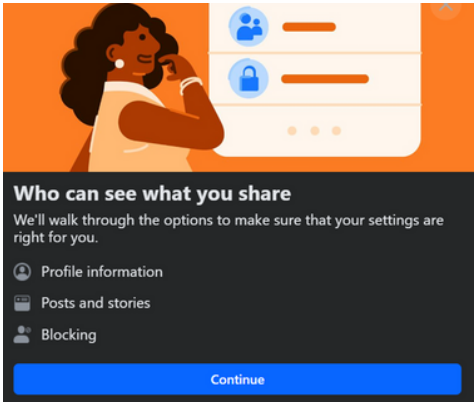


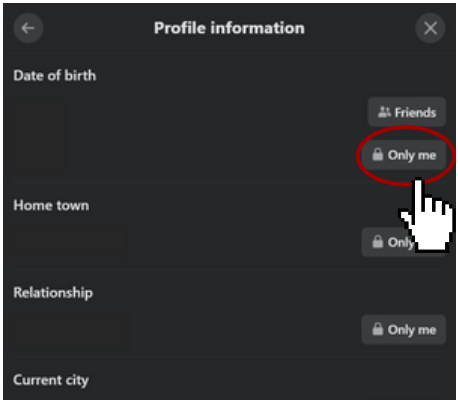
Facebook (Meta)

Once on the Privacy Check-up tool, you can click through each section to review and adjust your privacy settings.



For example, "Who can see what you share" takes you through your profile information, posts and stories, and blocked accounts. From here you can check who can view your personal information and the posts you share.

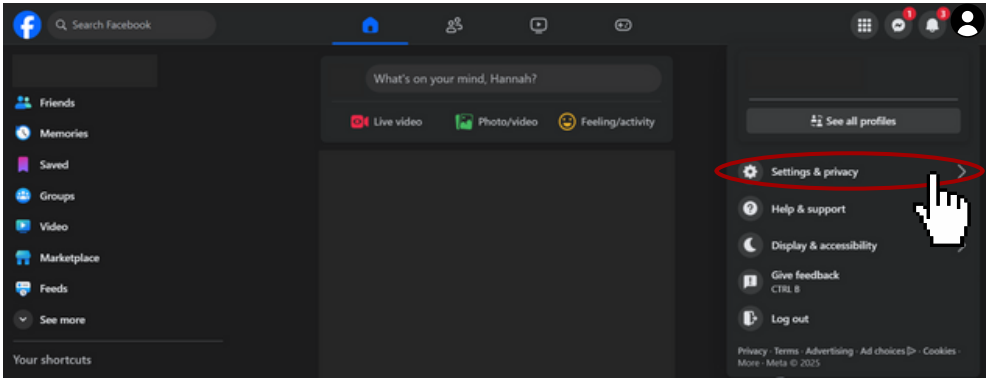


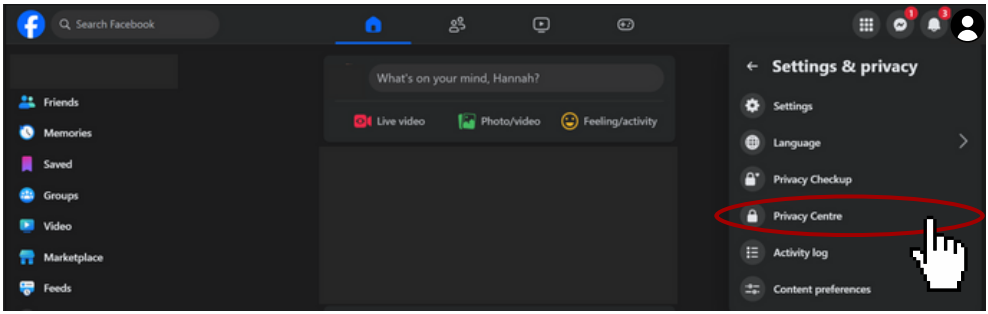


Facebook (Meta)

With regards to Security settings, the Privacy Check-up tool offers a section on "How to keep your account secure" which discusses aspects such as passwords and login alerts.

For a more detailed view of Security settings, Meta offers a Privacy Centre which can be navigated to under 'Settings & Privacy'.





By navigating to "Common privacy settings" you can manage your account details and security.

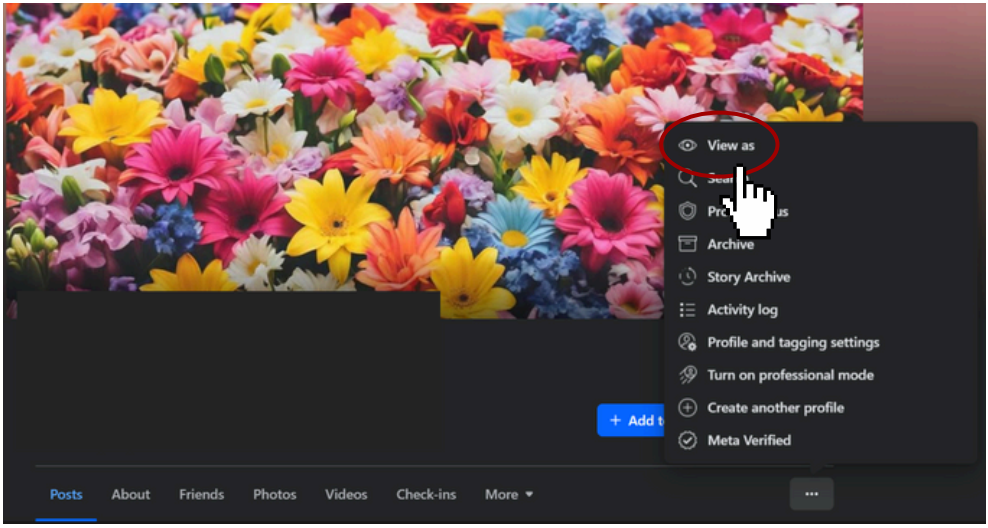
Here you can change your password, enable Two-Step Verification (2SV), and view login alerts.

Please see page 4 & 5 to understand why strong passwords and 2SV are important for your social media accounts.

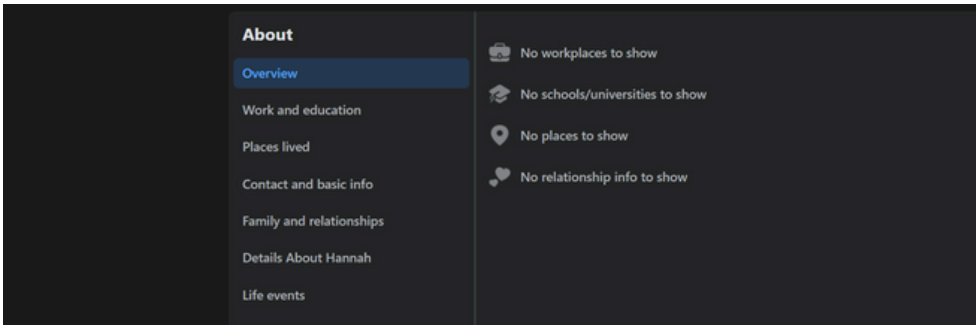
Facebook (Meta)

It is also good practice to see what information on your profile is public.

This can be done by navigating to your Facebook profile, clicking the three dots, and selecting “View As”. This will allow you to view what information on your profile is public.



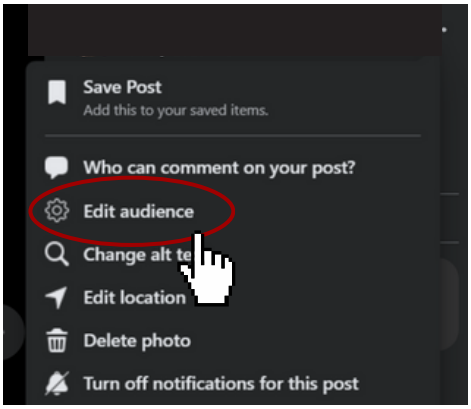
From here you can view and amend information which is shared publicly. Remember that any public information can be downloaded and shared outside of your profile.

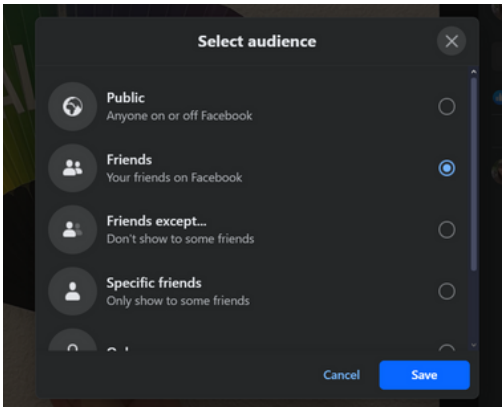


Facebook (Meta)

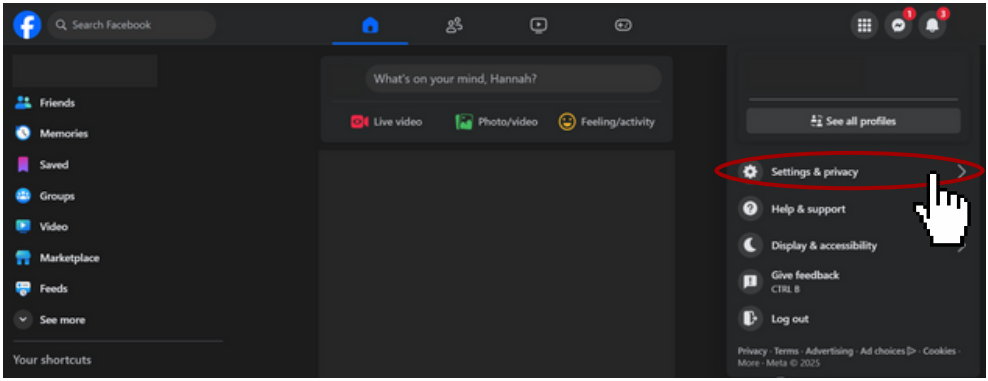
If you are not happy with the public information on your profile, review and amend your Privacy Settings.

You also have the option to control and modify who can view each of your posts directly. By selecting the three dots on the post, you can choose the “Edit audience” option.

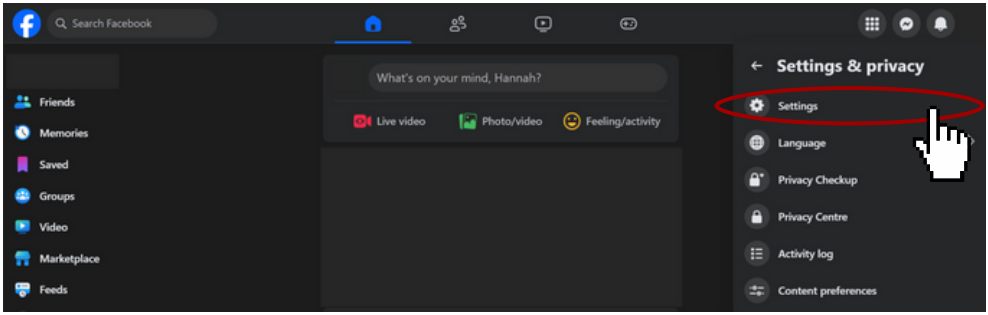




You can change who can see your previous posts.
To enhance your privacy on Facebook, use the Limit Past Posts feature to restrict old posts to "Friends" only. This prevents strangers from viewing your past content and helps protect your personal information. To do so first navigate to “Settings & Privacy” followed by “Settings”.

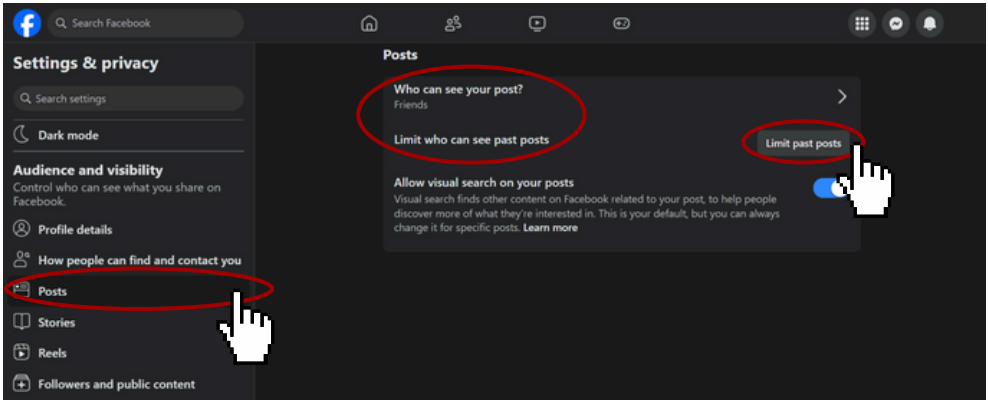


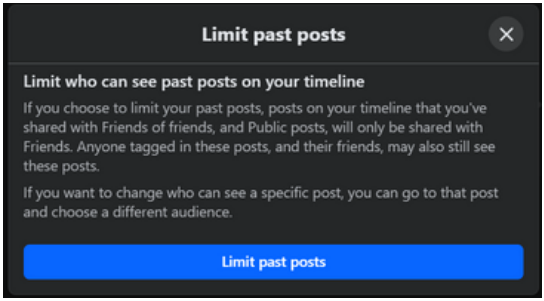
Facebook (Meta)



Following this, scroll down the panel on the left side of the page, until you reach the "Audience and Visibility" section. From here select "Posts" and you be able to limit your past posts to Friends, Friends Except, Specific Friends, Public, or Only Me. Select the option from the drop down, and click the "Limit past posts" button.

This will update the visibility of all previous posts at once, saving you from manually adjusting each one.



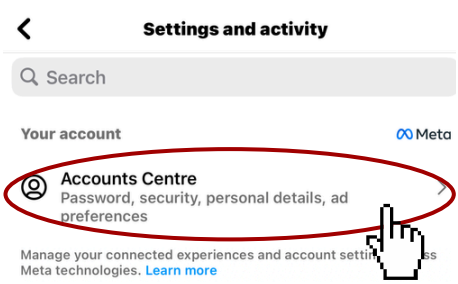


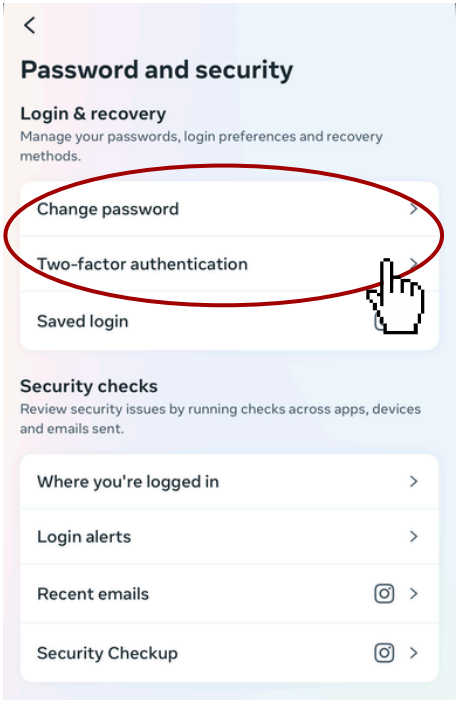
Instagram (Meta)

Instagram also has the same Account Centre as Facebook, as both are managed by Meta.

In the Accounts Centre you can amend your password, security settings, personal details, and preferences.

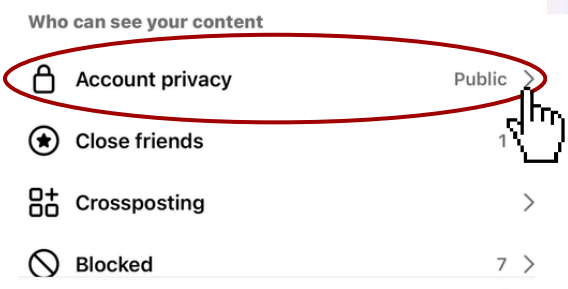
Once in the Accounts Centre you can navigate to 'Password and security' to amend your password, view security alerts, and enable two-factor authentication (2FA).





Privacy settings on Instagram are different from those on other platforms. By default, posts on Instagram are set to be public, meaning anyone can view them. However, you can amend this by changing your profile to private. When your profile is set to private, only your approved followers will be able to see your posts. This helps you control who can view your content, ensuring that your personal moments are shared only with your chosen audience.

You can make your profile Private by navigating to "Account privacy" in the Settings.

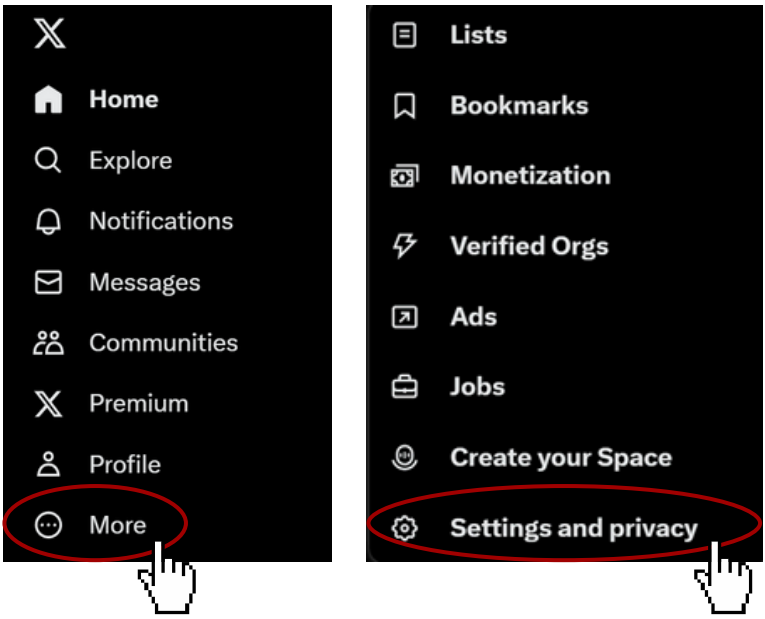


X (formerly Twitter)

X, formerly known as Twitter, is a platform for real-time conversations. To ensure a secure experience, X offers a comprehensive Settings and Privacy Centre.

On X, posts and profiles are public by default. This means that anyone can see your tweets and profile information. However, you can change your settings to make your account private. By doing this, only your approved followers will be able to see your tweets. This feature allows you to control who has access to your posts and personal information, ensuring a more private and secure social media experience.

Privacy Settings can be accessed by clicking 'More' followed by 'Settings and privacy'.



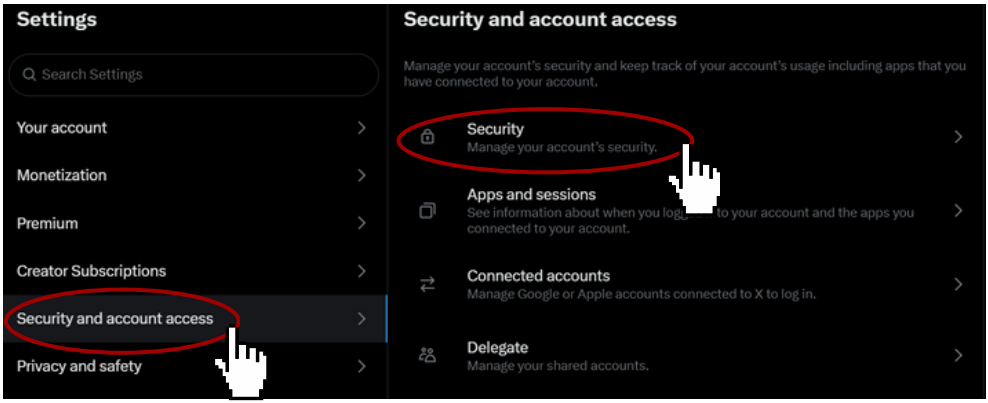
From here you will see:

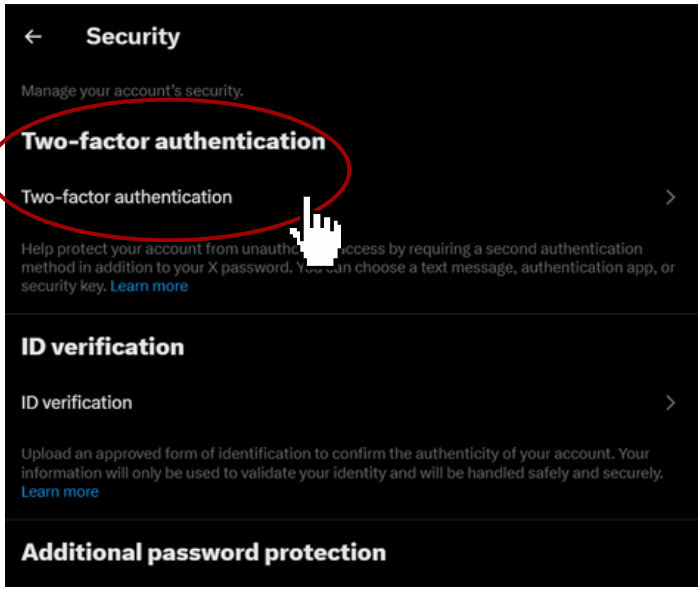
- Security and account access
- Privacy and safety

X (formerly Twitter)

'Security and account access' allows you to manage your account security.

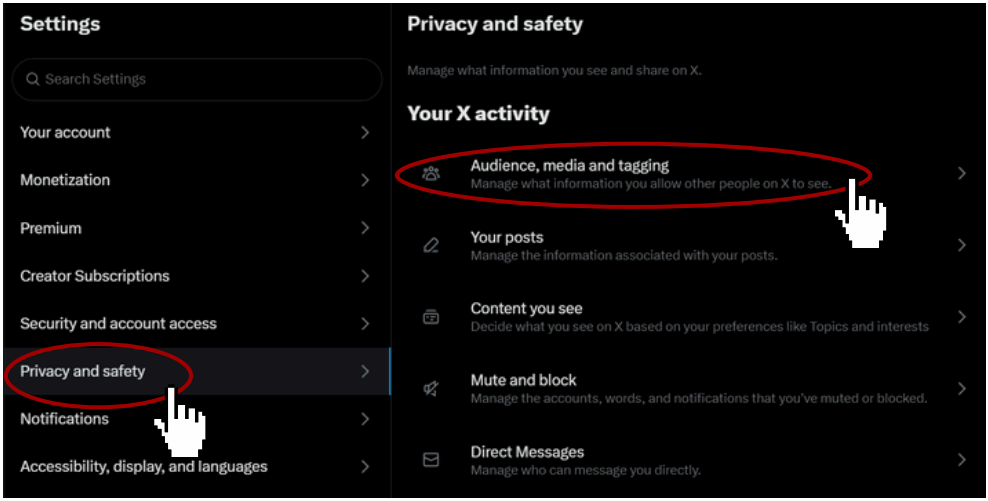
Under 'Security' you can enable two-factor authentication (2FA) and additional password protection.





X (formerly Twitter)

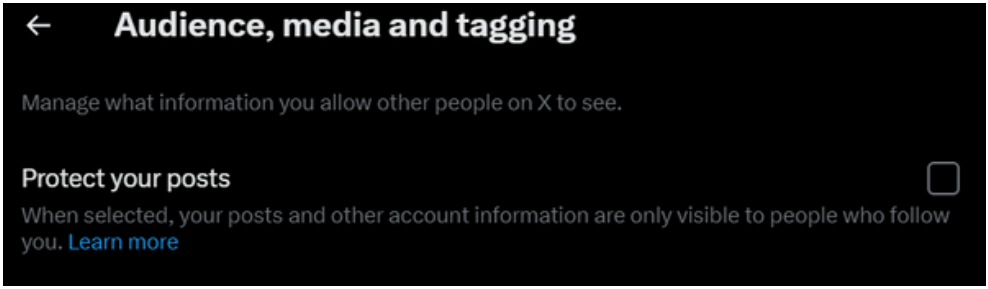
'Privacy and safety' allows you to view and manage who can view your profile, and the information you post.



For example under 'Audience, media and tagging' you can 'Protect your posts' which prevents people who are not following you from viewing your posts.

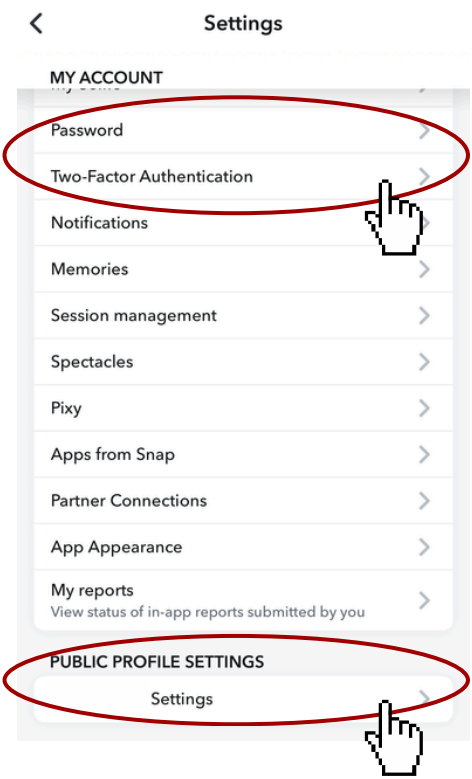
If you protect your posts, you'll receive a request when new people want to follow you, which you can approve or deny. Accounts that began following you before you protected your posts will still be able to view and interact with your protected posts unless you block them.

You can also control who can send you private messages under 'Direct Messages'.



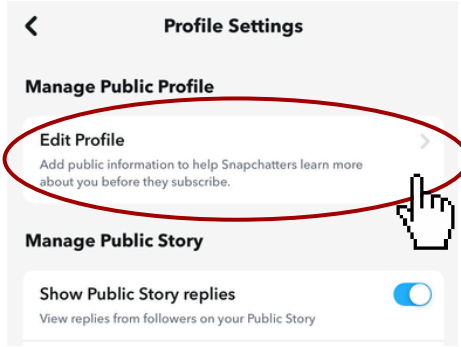
Snapchat

Snapchat, a multimedia messaging app known for its creative filters and unique features, enhances your social interactions. However, with these fun elements comes the importance of managing your privacy and security settings.

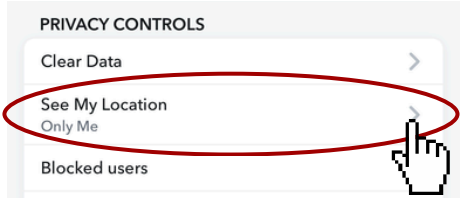


In the Settings you can manage your Security controls, for example by enabling two-factor authentication, changing your password, and managing your account/profile settings.

Under 'Public Profile Settings' you can edit your public information and manage your public stories.



Importantly, under 'Privacy controls' you can manage who can view your location. This is particularly important for Snapchat, which has the Snap Map feature.

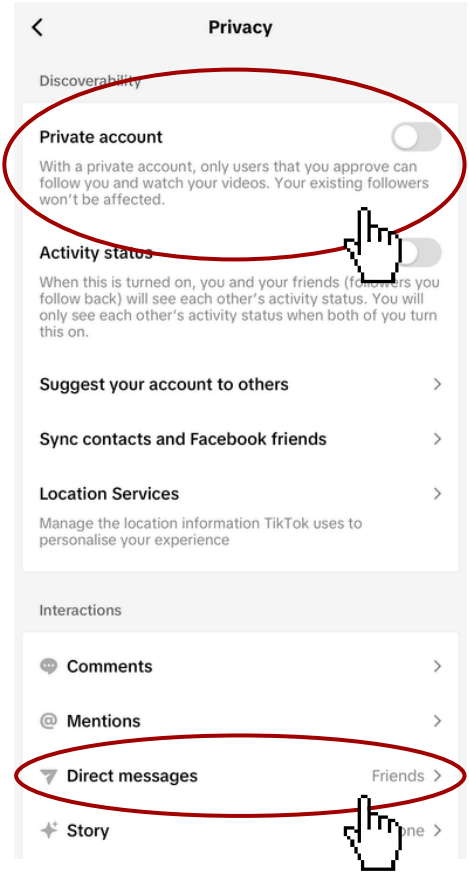


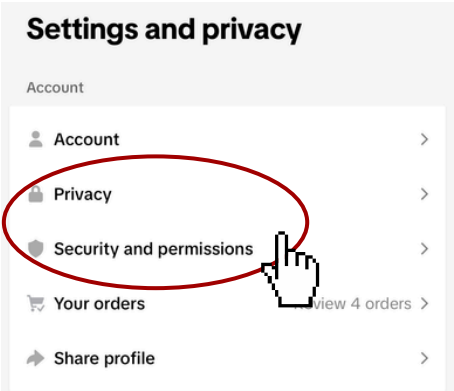
TikTok

TikTok, a rapidly growing platform known for its short, engaging videos, offers a creative space for users to express themselves and connect with a global audience. As you enjoy the diverse content on TikTok, it's important to understand and manage your privacy and security settings to safeguard your personal information.

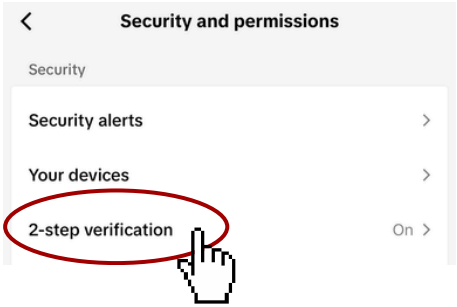
On TikTok, posts are typically set to be public, meaning anyone can view them. However, you have the option to make your profile private. By doing this, only users you approve can see your content, allowing you to control who has access to your videos and personal information, ensuring a more secure and private experience on the platform.

You can make your profile private by navigating to 'Privacy' in the Settings then selecting 'Private account'. Under this same section you can amend other privacy settings such as who can direct message you.





You can also manage your security settings under 'Security and permissions' with the option to enable two-step verification.

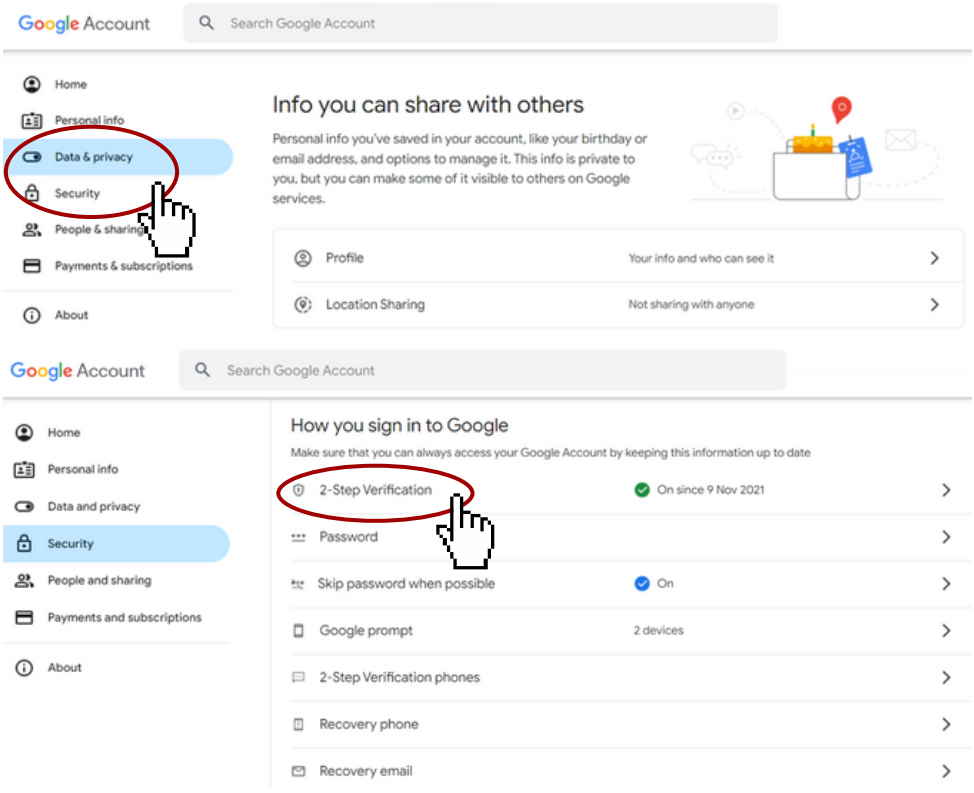


YouTube (Google Account)

YouTube, a leading platform for video sharing and streaming, is managed through your Google account. This integration allows for a unified experience across various Google services, making it easier to control and manage your privacy and security settings in one place.

By utilising your Google account, YouTube ensures that your preferences and settings are consistent across all Google platforms, providing a streamlined approach to managing your personal information.

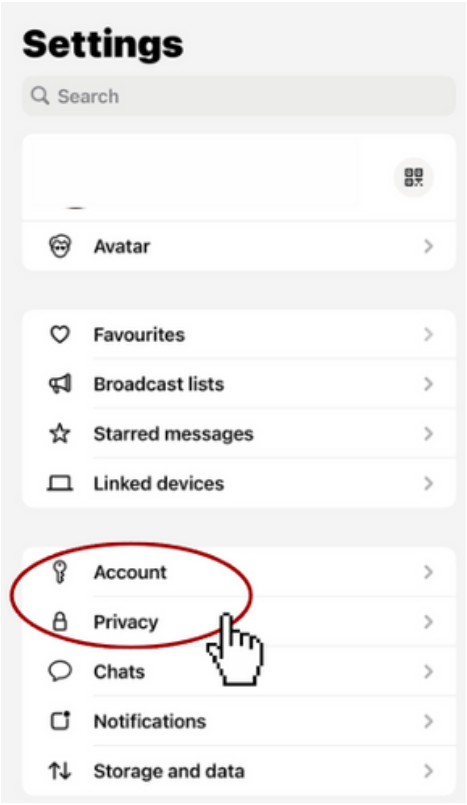
'Data & privacy' allows you to control who can view your Google profile and location sharing.
'Security' is where you can enable two-factor authentication, amend your password, and adjust other security settings, for example adding a recovery email.

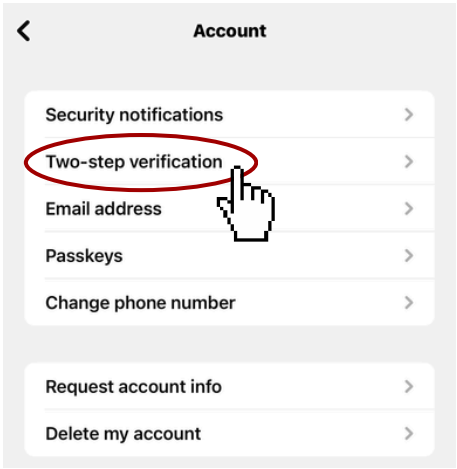


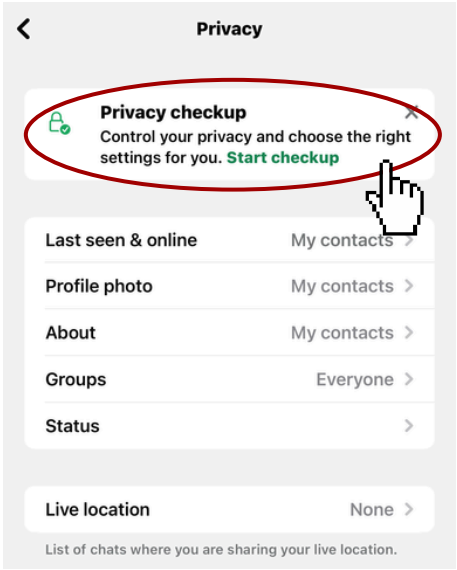
WhatsApp

WhatsApp, a popular messaging app owned by Meta, is known for its simplicity and reliability in connecting people worldwide. With its end-to-end encryption, WhatsApp ensures that your messages, calls, photos, and videos are secure and can only be seen by you and the person you're communicating with.

In the Settings under 'Account' security settings can be managed. Here you can enable security notifications and activate two-step verification.
Under 'Privacy' you can carry out a 'Privacy checkup' and manage how your personal information is shared.







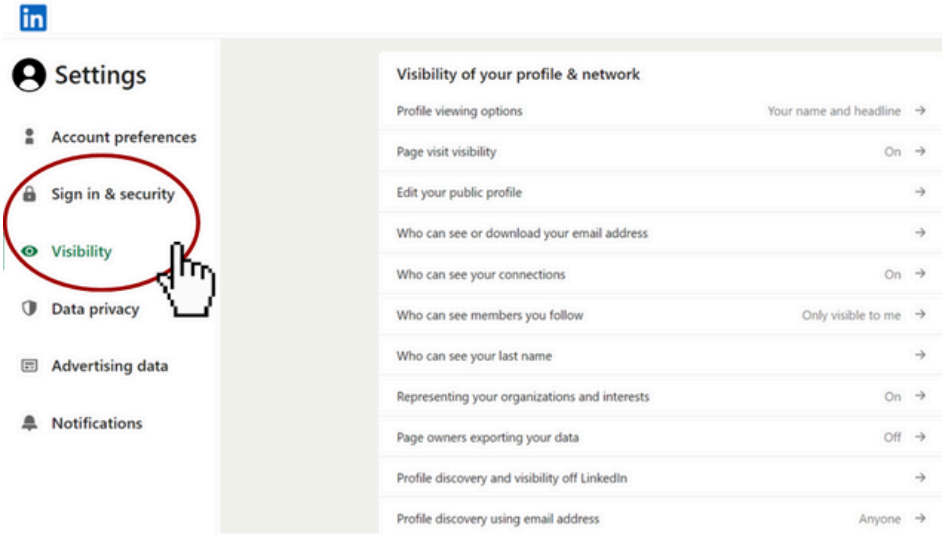
LinkedIn

LinkedIn is the premier social media platform for professional networking, career development, and industry insights. As you build and maintain your professional profile, it's important to be aware of and manage your privacy settings to ensure your information is shared appropriately.

LinkedIn offers a range of privacy and security features that allow you to control who can see your profile, posts, and activity. By customising these settings, you can protect your personal information and maintain a professional presence that aligns with your career goals. In this section, we'll guide you through the key settings and tools to help you navigate LinkedIn with confidence and peace of mind.

In the Settings under 'Visibility' you can control who can view your personal information, page visibility, connections, and more.

You can also view and amend your privacy settings under 'Data privacy'.



Find Out More

Staying safe online can sometimes feel overwhelming, but you don't have to navigate it alone. Below are some useful links and resources that provide additional information and support on various topics related to online safety. Whether you're looking for guidance on protecting your personal information or understanding the latest scams, these resources can help you stay informed and secure.

WWW.DEVON-CORNWALL.POLICE.UK/CYBER

The Devon and Cornwall Police Cyber Crime Unit homepage contains useful information and links to resources to help keep you safe online. You can also request tailored cyber awareness sessions covering a variety of topics.

WWW.NCSC.GOV.UK/CYBERAWARE

The National Cyber Security Centre (NCSC) is part of GCHQ (Government Communications Headquarters), the government's intelligence and security organisation. As such, they are well placed to provide impartial security guidance. Their Cyber Aware campaign gives straightforward advice to help people secure their accounts and defend against some of the more prominent forms of cybercrime.

WWW.ACTIONFRAUD.POLICE.UK

Action Fraud is the UK's national reporting centre for fraud and cybercrime in England, Wales and Northern Ireland. Should you fall victim, you should report to Action Fraud by visiting their website or by calling 0300 123 2040.

WWW.STOPTHINKFRAUD.CAMPAIGN.GOV.UK

Stop, Think Fraud is a National campaign offering straightforward, impartial advice that helps prevent email, phone-based, and online fraud. Stop, Think Fraud is brought to you by the UK Government in partnership with City of London Police, the National Cyber Security Centre, and the National Crime Agency.