SCHILLINGS

SOCIAL MEDIA PRIVACY GUIDE

Contents

INSTAGRAM

Make your account private

Once the private setting is activated, your pictures and videos will be hidden from non-followers and won't be displayed in public search results. You will also now be able to accept or deny follower requests.

- Navigate to **Settings** > tap **Privacy** > go to **Account Privacy** > toggle on the **Private Account** setting to make your account private.

Enable Two-Factor Authentication

- Navigate to **Settings** > go to **Security** > select **Two-Factor Authentication** > click or tap **Get Started** > choose how you want to get codes: receive via Text Message or generate in the Authentication App.

Turn your location off

- Leave the Instagram app and go to your iPhone's Settings > tap **Privacy** > go to **Location Services** > scroll down and tap **Instagram** > select **Never** or **While Using the App** to choose location access.

Unlink to other social media, including Facebook, Twitter and Tumblr

- Navigate to **Settings** > tap **Account**, then tap **Linked Accounts** > tap **Facebook**, and then tap **Unlink Account (iPhone)** or **Unlink (Android)** > tap **Yes, Unlink** to confirm.

Check Instagram emails to avoid phishing

- Navigate to **Settings** > tap **Security** > select **Emails From Instagram** > search through messages in the **Security** tab if it's about login attempts, suspicious activity on your account, and so on. If it's about something else, check the **Other** tab.

Choose who can see your Instagram stories

- Navigate to **Settings** > go to **Privacy** > click on **Story** > tap on **Close Friends** > here you can choose who to share your stories with.

Disable the resharing of your stories

- Navigate to **Settings** > go to **Privacy** > click on **Story** > scroll down to **Sharing** > here you can enable or disable sharing as message, and sharing your story to Facebook.

Block an inappropriate user

NB: blocked users can still see your likes and comments on mutual friend's images. They can also mention you via your username, and you will be notified of such a tag:

- Tap their username to go to their profile > tap the three dots in the top right > tap **Block/Unblock** this user > tap **Block/Unblock** again to confirm.

Hide from specific users

You can block or restrict certain spammers and other intrusive users from accessing your account.

- Tap their username to go to their profile > tap the three dots in the top right > tap **Restrict**.

Block spam in direct messages

- Navigate to **Settings** > go to **Privacy** > choose **Messages** > tap **Only People You Follow** for both options on the screen.

Block spam comments

- Navigate to **Settings** > go to **Privacy** > Tap on **Comments** > there you can choose who to block from commenting on your photos and videos.

Hide your activity status

If you don't want readers to know when you're online, you can hide your online status from them. Note that you too will be unable to see other users' online status.

- Navigate to **Settings** > go to **Privacy** > select **Activity Status** > slide the toggle to the off position.

Decide who can message you

When someone you aren't following tries to contact you, their messages get sent to a "message requests" tab. You can decide not to receive these messages at all.

- On your phone, go to your profile by clicking the icon in the bottom right. Open the menu in the top right, go to **Settings** > tap **Privacy** > scroll down to **Messages**. For the various potential connections, tap and select how you want to be contacted and who can add you to groups.

Prevent the use of your account for the expansion of Instagram's network

When users follow a new account, Instagram then recommends a few similar users. You can opt out of your account being suggested.

- Log in to Instagram on your computer. Click on your profile picture in the top right to open the menu and go to **Settings**. Click **Edit Profile** and scroll down to uncheck the box for **Similar Account Suggestions.**

WHATSAPP

Turn on Screen Lock/Fingerprint or Face ID

- Open WhatsApp on your phone and go to **Settings** > **Account** > **Privacy** > select **Screen Lock** > enable it. Your app will now require you to enter your screen lock before it launches.

Stop sharing your live location

- Go to > **Settings** > **Account** > **Privacy** > **Live location** > click **STOP SHARING** > **STOP**.

Restrict who sees your Profile Picture/ Status

- Go to **Settings** > **Account** > **Privacy** > **Profile Photo**, and choose from **Everyone**, **My Contacts** and **Nobody**.
- Change who has access to your status updates through the Privacy tab. Choose from **My Contacts**, **My Contacts Except...** or **Only Share With...**.

Turn off Read Receipts (aka the blue ticks)

Read receipts can be turned off if you do not want your contacts to know whether you have read their messages or not. Once you turn off read receipts, you will not be able to view other people's read receipts either.

- Go to **Settings** > **Account** > **Privacy** > **Read Receipts** and then turn on/off the toggle. In Groups, your read receipts will always show even with the option turned off.

Turn off Photo Backups

Photos received through WhatsApp are stored in your phone's camera roll. If you use iCloud or Google Drive to back up images on your phone but do not want to do so for WhatsApp, you can turn that off.

- Go to **Settings** > **Chats** > **Save to Camera Roll**. From there, you can toggle the switch to **off** if you don't want the photos and videos you receive saved to your phone's camera roll.

Delete your WhatsApp Status

If you wish to, you can delete your WhatsApp Status.

- On iPhone, tap on **My Status** and swipe left on a status to reveal the **Delete** button. Next, tap **Delete** from the pop-up.

- On Android, go to the Status section, tap the three-dot menu adjacent to **My Status**, select the same button adjacent to the status you want to delete, and select **Delete**. Tap **Delete** again to confirm.

Turn off Chat Backups

It is recommended to disable backups to ensure the privacy of your data. Your backed-up data can be accessed by Apple or Google. However, there have been no serious claims that users' content in the cloud has been analysed or datamined by these companies.

- Go to **Settings**, select the **Chats** option, and go to **Chat Backup**. Tap on **Auto Backup** and select **Off**. Once this is done, your WhatsApp data will stop backing up on iCloud. You have the liberty to turn the backup option **On** whenever you wish to. Once the Chat Backup option is set to **Off**.

- Within WhatsApp, go to your iPhone's System Settings and tap on the **Apple ID, iCloud, Media and Purchases** banner at the top of the screen. Go to **iCloud**, then **Manage Storage**, then **WhatsApp**, and finally **Backup**. From there you can make sure the backup option is off as well. You also have the possibility to delete old chats by clicking on **Delete All**.

Hide your About information

When clicking on a contact in WhatsApp, it is possible to see a short bio or a statement, or just an away message. It is up to users to make this 'About' information private.

- Go to **Settings** > **Account** > **Privacy.** Tap on **About** and choose between **My contacts** or **Nobody** to make sure your **About** information is not public. Additionally, you can also choose to make your **Last Seen** and **Profile Photo** private from the **Privacy** tab. The process to do so is similar to the **About** information.

Unlink your account from devices

If someone has your WhatsApp account on their laptop, you have the possibility to log out from all devices through your phone.

- On Android, stay on the Chat section, click on the three-dot menu in the top right corner. Tap on **Linked Devices**. Tap on each device to log out.
- On iPhone, go to **Settings** and then **Linked Devices**. Next, tap **Log out** from all devices to log out.

LINKEDIN

Manage your Profile Information

- **Desktop:** Navigate to **Settings and Privacy** > go to **Account preferences** in the left column > click **change** next to **Name, location, and industry**. From there you can choose how your name and profile fields appear to other members.
- **Mobile phone:** Navigate to **Settings** > go to **Account preferences** > tap on **Name, location, and industry**. From there you can choose how your name and profile fields appear to other members.

Stop syncing your contacts

- **Desktop:** Navigate to **Settings and Privacy** > go to **Account preferences** in the left column > scroll down to **Sync contacts** and click **change**. From there, click on **Remove all**.
- **Mobile phone:** Navigate to **Settings** > go to **Account preferences** > Scroll down to **Syncing options** and click on **Sync contacts**. From there toggle off the option and remove all previously synced contacts.

Don't send your data to Microsoft and Twitter

- **Desktop:** Navigate to **Settings and Privacy** > go to **Account preferences** in the left column > scroll down to **Partners & Services** > click **change** next to **Microsoft** and **Twitter** > tap **Remove**.
- **Mobile phone:** Navigate to **Settings** > go to **Account preferences** > scroll down to **Partners & Services** > click on **Microsoft** and **Twitter** respectively and tap **Remove**. (If you've connected your Twitter account to LinkedIn, you can remove that from this same tab as well.)

Turn on Two-Factor Authentication

- **Desktop:** Navigate to **Settings and Privacy** > choose **Sign in & security** on the left rail > click on **Change** next to **Two-step verification** > click **Turn on** to change the status of two-step verification. You may be asked to enter your password for security reasons.
- **Mobile phone:** Navigate to **Settings** > go to **Sign in & security** > scroll down and select **Two-step verification** > click on **turn on** > and choose a verification method. You can choose between an authenticator app or SMS (text) messages. You may be asked to enter your password for security reasons.

Deactivate Remember Me

- **Desktop:** Navigate to **Settings and Privacy** > go to **Sign in & security** on the left rail > click on **Change** next to **Devices that remember your password** > choose **Remove all Devices** or remove each device individually.
- **Mobile phone:** Navigate to **Settings** > click on **Sign in & security** > scroll down and select **Devices that remember your password** > choose **Remove all Devices** or remove each device individually.

Secure your LinkedIn phone app

- Navigate to **Settings**> click on **Sign in & security** > scroll down and select **App lock** > turn on **App lock**.

Block sponsored messages

- **Desktop:** Navigate to **Settings and Privacy** > click on **Data Privacy** > scroll down to **Messages** > Switch off the toggle under **Allow LinkedIn partners to show you Sponsored Messages**.
- **Mobile phone:** Navigate to **Settings** > click on **Data Privacy** > scroll down to **Messages** > Switch off the toggle under **Allow LinkedIn partners to show you Sponsored Messages**.

Choose how your profile appears to non-logged in members

- **Desktop:** Navigate to **Settings and Privacy** > go to **Visibility** in the left rail > under **Visibility of your profile & network**, click on **Change** next to **Edit your public profile** > toggle **Your profile's public visibility** to **Off**.
- **Mobile phone:** Navigate to **Settings** > tap on **Visibility** > select **Edit your public profile** > go to **Edit Visibility** and turn off **Your profile's public visibility**.

Hide your last name

- **Desktop:** Navigate to **Settings and Privacy** > go to **Visibility** in the left rail > under **Visibility of your profile & network**, click on **Change** next to **Who can see your last name** > there you can choose between your full name or having the first initial of your last name.
- **Mobile phone:** Navigate to **Settings** > click on **Visibility** > tap on **Who can see your last name** > there you can choose between your full name or having the first initial of your last name.

LINKEDIN

Control your profile's visibility off LinkedIn

- **Desktop:** Navigate to **Settings and Privacy** > go to **Visibility** in the left rail > under **Visibility of your profile and network**, click on **Change** next to **Profile visibility off LinkedIn** > turn off the setting.
- **Mobile phone:** Navigate to **Settings** > tap on **Visibility** > click on **Profile visibility off LinkedIn** > turn off the setting.

Control who can find you using your email address

- **Desktop:** Navigate to **Settings and Privacy** > go to **Visibility** in the left column > under **Visibility of your profile & network**, click **Change** next to **Profile discovery using email address** > select the **Nobody** option.
- **Mobile phone:** Navigate to **Settings** > tap on **Visibility** > go to **Profile discovery using email address** > choose 1st degree connections.

Control who can find you using your phone number

- **Desktop:** Navigate to **Settings and Privacy** > select **Visibility** in the left column > under **Visibility of your profile & network**, click **Change** next to **Profile discovery using phone number** > select the **Nobody** option.
- **Mobile phone:** Navigate to **Settings** > go to on **Visibility** > tap on **Profile discovery using phone number** > select **Nobody**.

Manage who can see your connections

- **Desktop:** Navigate to **Settings and Privacy** > go to **Visibility** in the left column > under **Visibility of your profile & network**, click **Change** next to **Who can see your connections** > select **Only you**.
- **Mobile phone:** Navigate to **Settings** > tap on **Visibility** > go to **Who can see your connections** > select **Only you**.

Manage Active Status

- **Desktop:** Navigate to **Settings and Privacy** > go to **Visibility** in the left column > under **Visibility of your LinkedIn activity**, click **Change** next to **Manage active status** > select **No one**.
- **Mobile phone:** Navigate to **Settings** > go to **Visibility** > scroll down to **Manage active status** > select **No One**.

Control mentions and tags

- **Desktop:** Navigate to **Settings and Privacy** > click on **Visibility** in the left rail > under **Visibility of your LinkedIn activity**, click **Change** next to **Mentions or Tags** > turn off the option.
- **Mobile phone:** Navigate to **Settings** > tap on **Visibility** > scroll down to **Mentions or Tags** > toggle the option off.

Review your Who's Viewed Your Profile settings

- **Desktop:** Navigate to **Settings and Privacy** > go to **Visibility** in the left-hand column > under **Visibility of your profile & network**, click on **Profile viewing options** > select **Private mode.**
- **Mobile phone:** Navigate to **Settings** > tap on **Visibility** > tap on **Profile viewing options** > select **Private mode.**

Review who can see or download your email address

- **Desktop:** Navigate to **Settings and Privacy** > go to **Visibility** in the left column > under **Visibility of your profile and network**, click on **Who can see or download your email address** > select **Only visible to me**, and toggle off the option for your connections to download your email in their data export.
- **Mobile phone:** Navigate to **Settings** > tap on **Visibility** > go to **Who can see or download your email address** > select **Only visible to me**, and toggle off the option for your connections to download your email in their data export.

Control the data collected on you

- **Desktop:** Navigate to **Settings and Privacy** > choose **Advertising data** in the left column > Click on **Profile data for personalising ads** and disable the option. Click on **Location** and disable the option. Scroll down to **Third-party data** and toggle off each option.

- **Mobile phone:** Navigate to **Settings** select **Advertising data** > Click on **Profile data for personalising ads** and disable the option. Click on **Location** and disable the option.Scroll down to **Third-party data** and toggle off each option.

TIKTOK

Pay attention to privacy features

- In your profile, tap the three horizontal buttons at the top right of the screen > Select **Privacy** >
  - Switch off **Suggest account to others**
  - Turn off **Sync contacts and Facebook Friends**
  - Turn off **Ads personalisation** and A**d authorisation**
  - Turn off **Downloads** to prevent others from downloading your videos
  - Restrict comments by choosing between Everyone, Friends, or Off
  - Limit who can Duet with your videos by choosing between **Followers, Friends** or **Only me**
  - Control who can send you direct messages by choosing between **Friends** or **no one**

Manage your devices

- In your profile, tap the three horizontal buttons at the top right of the screen > Select **Security and Login** > Go to **Manage Devices** and remove the devices you are no longer using.

Turn on two step verification

- In your profile, tap the three horizontal buttons at the top right of the screen > Select **Security and login** > Go to **2-step verification**, choose your verification method and then follow the instruction on the screen.

Don't save login information

- In your profile, tap the three horizontal buttons at the top right of the screen > Select **Security** and login > toggle off **Save login info**.

Use Parental Controls to restrict screen time and content type

- Go to your profile in the bottom right corner > Tap the three buttons in the top right corner > Tap **Settings and Privacy** > Tap **Content Preferences** > Select **Restricted Mode** and turn setting **on**.

- Go to your profile in the bottom right corner > Tap the three buttons in the top right corner > Tap **Settings and Privacy** > Tap **Screen time** > Tap **Daily Screen Time** and turn setting **on**.

Manage Family Pairing controls by linking parents and teen accounts

- Go to your profile then tap the three dots located in the top right-hand corner > Go to **Family Pairing** then follow the on-screen instructions > Once you pair the accounts, simply select the account you want to manage and update the controls.

Make an account private

TikTok accounts are public by default, which means anyone can see what you're posting.

- In the profile, tap the three horizontal buttons at the top right of the screen > Select **Settings and Privacy** > Select **privacy** > turn on **private account.**

ZOOM

Don't use your Personal Meeting ID for meetings

Instead, use the auto generation of per-meeting ID, exclusive to a single meeting. Recycle your meeting IDs so the same ID and password isn't used for another meeting.

- Keep the meeting ID to those only invited and make sure all of your meetings have a password.

What to do if someone interrupts your Zoom video chat

- Lock them out. Go to the **Participants List** in the navigation sidebar and scroll down to **More**. Click **Lock Meeting** to stop further participants from entering the meeting and to be able to remove participants.

- Mute them. Have yourself or one of your co-hosts go to the **Participants List**, again scrolling down to the bottom, and click **Mute All Controls**. This makes it so the unwelcome participant can't use their microphone to disrupt your audio.

Update meeting settings to protect your privacy

We recommend ensuring the following settings are altered to protect your session against unwanted visitors. To do so, follow these steps:

- Once logged in to the Zoom portal > head to **Settings** under **Personal** > click on **Meeting**. You should then be able to find the settings below by scrolling down the list of settings under the **Meeting** section. While in a meeting, some privacy settings can be adjusted via the **Share Screen** button, but most control is offered in the web portal's **Settings** menu.

- Turn on the **Require that All Meetings are Secured with One Security** option. This will require that all meetings are secured with one security option: a passcode, **Waiting Room**, or **Only authenticated users can join meeting**s. If no security option is enabled, Zoom will secure all meetings with **Waiting Room**.

- Enable the **Waiting Room** feature so that only the meeting host is allowed to admit attendees to the meeting.

- Enable the **Meeting Passcode** option so that all instant and scheduled meetings are passcode-protected.

- Turn on the **Only Authenticated Users Can Join Meetings from Web Client feature** so that participants have to authenticate prior to joining meetings from web client.

- Disable the **Allow Participants to Join Before Host** option to prevent participants from joining the meeting before the host arrives.

- Disable the **Auto Saving Chats** option to avoid automatically saving all in-meeting chats after the meeting starts.

- Disable the **Send Files via Meeting** chat option to prevent the spread of unwanted material.

- Adjust your Screen Sharing settings. It is possible to disable screen sharing entirely, or to limit it to just the host by selecting **Host Only** under **Who Can Share?**

- Disable the **Annotation** option to prevent host and participants from using annotation tools to add information to shared screens.

- Disable the **Allow Removed Participants to Rejoin** option so that any unwanted visitors can't access the video call once removed.

AMAZON

Enable Two-Step Verification

- Click on **Account & Lists** in the top right of the screen > go to **Your Account** > tap **Login & Security** > go to **Manage your Two Step Verification** (2SV) **Authenticators** and click **Edit**. You will need to approve the notification sent to your email address. Once this is done, click on **Get Started** button.

The process is automated, so you just need to follow the prompts to activate the 2SV. First, you will need to enter your phone number and then will receive the first code. Once you've verified the first code, you will need to set a backup method. This can be a text or voice call on a different phone, or an authenticator app. Lastly, read the instructions on what to do on devices that won't work with two-step verification. Once you're all finished, you can tick the box to skip asking for codes on this device – it is recommended doing this only if it's a desktop, which is much less likely to get stolen than something like a laptop or tablet.

Clear Amazon cookies

- Click on **Accounts & Lists** > go to **Your Account** > tap on **Browsing History** in the horizontal banner at the top of the screen > click **Manage History** on the right side of the screen > select **Remove all items** and then switch off **Turn Browsing History on/off**.

- Click on **Accounts & Lists** > under E**mail alerts, messages, ads, and cookies**, tap on **Advertising preferences** > select **Do not show me interest-based ads provided by Amazon** > then click **Submit**.

- Click on **Accounts & Lists** > under **Email alerts, messages, ads, and cookies**, tap on **cookie preferences** > next to **Advertising cookies**, choose **Off**.

Hide your order history

It isn't possible to permanently delete your order history, but you can archive orders and hide them from view.

- Click on **Account & Lists** > go to **Your Account** > select **Your Orders** section > next to each of your orders, click **View order details** > choose **Archive order** for the items you want to hide. A yellow box will appear asking you to confirm the change. Click on the yellow **Archive order** button to remove the item from your orders list.

Make your wish lists private

- Go to **Accounts & Lists** > select **Your Lists** in the scroll down menu. In the left side of the screen is a list of your lists and their privacy levels. If you see a public list that should be private, select the list and then click the 3-dot menu icon and select **Manage list** and change the privacy setting to **Private**. Once done, click **Save Changes**.

Delete Alexa recordings

Alexa is listening, but you can stop the smart speaker from holding on to everything it records. Deleting your recordings prevents Amazon from hearing your private conversations but be warned it may also affect Alexa's ability to understand you as well.

- To go further, you can set up Alexa to automatically delete future recordings via voice command. To do so, go to your Alexa app, log in and go to **Settings**, followed by **Alexa Account** > select **Alexa Privacy**, then **Review Voice History** > slide the toggle to the right that says **Enable deletion by voice**. Once this is done, you can ask Alexa to delete your recordings by saying, "Alexa, delete everything I said today."

Secure your account

If you think your Amazon account has been compromised, it is possible to take steps to make your account more secure.

- Click on **Account & Lists** > go to **Your Account** > tap **Login & Security** > go to '**noticed suspicious account activity?**' and click **Start**. Once this is done, you will be presented with three steps to secure your account.

- **Step 1** is updating your email settings. Amazon recommends changing your password to a strong, unique password that hasn't been used anywhere else and checking for 'email forwarding' rules and remove any if found.
- **Step 2** is setting a mobile PIN/passcode. Amazon recommends contacting your mobile phone provider and adding a PIN/passcode to protect your mobile phone account.
- **Step 3** is signing out all apps, devices and web browsers. For maximum security, it is recommended to sign out of everything. Once you have completed these steps, click on **Done** button.

FACEBOOK

Hide your location

Facebook uses your location data to target the daily news and suggestions you receive on the app. Even if you disable your location services in your mobile phone settings, Facebook still has access to your network location. It is essential to disable location tracking on both your device and in the Facebook app to hide your location.

- To disable location services on an iPhone: go to the phone's **Settings** > **Privacy**. Tap on **Location Services** > **Facebook**. From there, tap **Never** to disable location services.
- To disable location services on an Android phone: go to the phone's **Settings** > **Privacy**. Go to **Permissions Manager** >**Location**. Choose **Facebook**. From there, tap **Deny** to disable location services.

Once you have adjusted your phone's permissions, follow the following steps to disable location tracking in the Facebook app:

- In the Facebook app, tap the icon with the three lines in the bottom right, scroll down to **Settings and Privacy > Privacy Shortcuts** > **Manage Your Location Settings** under **Privacy**, followed by **Location Services**. Toggle off the **Location History** settings.

Enable Two-Factor Authentication

- **Desktop:** Click your profile picture in the top right of the screen and click on **Settings and Privacy > Settings** > **Security and Login** in the left column. Scroll down to **Two-Factor Authentication** and tap on **Use two-factor authentication.** Enter your phone number. A six-digit code will be sent to your device. Confirm the code in the text box to complete the setup.

- **Mobile phone:** In the Facebook app, select the three horizontal dots menu icon in the bottom right corner of the screen. Scroll down and tap on **Settings and Privacy.** In the dropdown menu, select **Account** > **Settings and security**. Scroll down to **Use two-factor authentication** select **Text Message (SMS)** as a security method. Enter your phone number and tap on **Continue**. A six-digit code will be sent to your device. Enter it in the text box and select **Continue**. Two factor authentication is now enabled on your account.

Limit what others can see

- **Desktop:** Once you are on the main Facebook page, click the downward-pointing arrow in the top right corner of the screen. Select > **Settings and Privacy** then go to > **Settings**. Go to > **Privacy** on the left menu. Review each setting to manage your defaults. To ensure full privacy, it is recommended that you choose between **Friends, Specific Friends and Only Me**.

- **Mobile phone:** In the Facebook app, tap the icon with the three lines in the bottom right. Scroll down to > **Settings and Privacy** and select > **Settings**. Go to > **Audience and Visibility**. Review each option and their respective settings to manage your defaults. To ensure full privacy, it is recommended that you choose between **Friends**, **Specific Friends** and **Only Me**.

Manage photo tagging

- **Desktop:** Once you are on the main Facebook page, click the downward-pointing arrow in the top right corner of the screen. Select > **Settings and Privacy** then go to > **Settings**. Go to **Profile and tagging** on the left menu. Review each setting to manage your defaults. To ensure full privacy, it is recommended that you turn off the setting or choose between **Friends** and **Only Me**.

- **Mobile phone:** In the Facebook app, tap the icon with the three lines in the bottom right. Scroll down to > **Settings and Privacy** and select > **Settings**. Go to > **Audience and Visibility**. Under **Profile and tagging**, review each setting to manage your defaults. To ensure full privacy, it is recommended that you turn off the setting or choose between **Friends** and **Only Me**.

Remove your account from Google

- **Desktop**: On the main Facebook page, click the profile picture in the top right corner of the screen. Click on **Settings and Privacy**, and then go to **Settings** > **Privacy** in the left column. Under **How people can find and contact you**, go to **Do you want search engines outside of Facebook to link to your profile?** and click on **Edit**. Uncheck the box on the bottom of the screen to turn off the setting.

- **Mobile phone:** In the Facebook app, tap the icon with the three lines in the bottom right, scroll down to **Settings and Privacy** and click on **Settings**. Go to **Audience and visibility** and tap on **How people can find and contact you.** Select **Do you want search engines outside of Facebook to link to your profile?** and disable the option.

FACEBOOK

Disable facial recognition

Facebook uses facial recognition to identify users that are present on photos posted on the platform. This explains why users are automatically tagged in photos that others post.

- **Desktop:** Once you are on the main Facebook page, click the downward-pointing arrow in the top right corner of the screen. Select > **Settings and Privacy** and then go to > **Settings**. In the left column, click on **Face Recognition**. Select **No** to the question **Do you want Facebook to be able to recognize you in photos and videos?** Facial recognition will be disabled for your account.

- **Mobile phone:** In the Facebook app, select the three horizontal dots menu icon in the bottom right corner of the screen. Scroll down to > **Settings and Privacy** and select > **Settings**. Go to > **Permissions** and click on > **Face recognition**. Select **No** to **Do you want Facebook to be able to recognise you in photos and videos?**

Limit Facebook advertisements

When your friends like an ad on Facebook, it's likely you'll see this ad too. And vice versa. Facebook automatically uses these ad's endorsements to tailor its advertising strategy to you and your friends. You can disable this tracking feature to keep your likes and dislikes more private.

- **Desktop:** On the main Facebook page, click the downward-facing arrow in the top right corner of the screen. Click on **Settings and Privacy**, and then go to **Settings**. Scroll down to **Ads** in the left column. There click on **Ad Settings** in the left column. Select each setting and deactivate them. Under **Social Interactions**, choose **Only Me**.

- **Mobile phone:** In the Facebook app, select the three horizontal dots menu icon in the bottom right corner of the screen. Scroll down and tap on > **Settings and Privacy**. In the dropdown menu, select > **Settings**. Under > **Permissions**, go to > **Ad preferences**. Select > **Ad settings** at the top of the screen. Select each setting and deactivate them. Under **Social Interactions**, choose **Only Me**.

Control your off-Facebook data

Facebook constantly monitors your activity, both on and off its site, as it helps the platform to send you targeted advertisements. It is possible to tailor or even delete this history data through the Off-Facebook activity page. To review and clear your Facebook history it is recommended that you log into your account on a desktop. It is possible to do it on mobile devices, but the process is more comprehensive on a computer.

- **Desktop:** Once on the main Facebook page, click on the downward-facing arrow in the top right corner of the screen, click on > **Settings and Privacy**, and then on > **Settings**. Go to > **Your Facebook Information** in the left column. Click on **view your Off-Facebook activity**. From this page, you can:

- Clear your history by clicking on the **Clear history** option. Please note this option is misleading. As although it disconnects your profile data from your account, stopping Facebook from targeting you with specific ads, it won't completely prevent Facebook from collecting analytics reports from the other websites you are visiting. You need to log out completely in order to prevent such data collection.

- Select the > **Manage future activity** option which is the permanent version of **Clear history**. When this option is turned off, companies are no longer able to supply Facebook with ad-targeting data on your online likes and dislikes. Please note that disabling **Future off-Facebook activity** will prevent you from signing into other apps and websites using Facebook.

- Click on the > **Manage your Off-Facebook activity** option which will show you the apps and sites that have shared ads with your Facebook account. When you're ready to clear this information, click **Clear History**.

- Choose to > **Download your information**. It is possible to download a copy of your Facebook information at any time. It can be a complete copy of your information, or specific types of information and date ranges that you wish to review. Downloading your information is a password-protected process that only you will have access to. Once your copy has been created, it will be available for download for a few days.

- **Mobile phone:** To clear your history, tap the three-line menu in the bottom right of the Facebook app, scroll down to > **Settings and Privacy**, and click on > **Settings**. Under > **Permissions**, go to > **Off-Facebook Activity** and open the tab. Examine the apps that monitor your online activity. Once you are sure you want to remove the information tap **Clear history**.

- Within the **Off-Facebook Activity** tab, click on **More options** and select **Manage Future Activity**. Click again on > **Manage Future Activity**, toggle off **Future off-Facebook activity** and click on **Turn off**.

FACEBOOK

Prevent apps from tracking you

When you connect to platforms or websites using your Facebook login details, you are granting those companies access to your personal data and allow them to share your online activity with Facebook. You need to use the desktop version of Facebook to disable this tracking feature.

- **Desktop:** Once you are on the main Facebook page, click on your **profile picture** in the top right corner of the screen. Select **Settings and Privacy,** and then go to **Settings**. Scroll down to **Apps and Websites** on the left menu. Select **Active**. Click on the box next to the app's name and click **Remove**. This will disable it and prevent the app from tracking your online activity.

SLACK

Enable Two-Factor Authentication

- **Via authentication app:** before you can set up 2FA on your account, you will need to download and install an authentication app on your device. Slack 2FA can be used with most Time-Based, One-Time Password (TOTP) applications. Once the authentication app has been downloaded, go to your **workspace** > go to your **Account** > tap on **Settings** > click **Expand** next to **Two-factor authentication** > click **Set up two-factor authentication** > enter your password > click **Use an app** to retrieve authentication codes from the authentication app on your device > add a new account. In most apps, you can do this by tapping the **+** icon > scan the QR code by using your device's camera. If you prefer, you can choose to enter the code by hand > on Slack's 2FA configuration page, enter the 6-digit verification code that your authentication app generates > to finish, press **Verify code**.

- **Via SMS text message:** sign in to your workspace > go to your **Account** > tap on **settings** > click **Expand** next to **Two-factor authentication** > click **Set up two-factor authentication** > enter your password > click SMS text message to receive authentication codes by text message > select your country from the menu, and enter your mobile phone number. Include your area and/or zone code > next, you will be sent a six-digit verification code to your device. Enter the code on the Slack 2FA configuration page > to finish, select **Verify code**.

Customise DMs and message retention

- If you are using Slack for work, it's likely that you are using a paid plan. This means that your supervisors may be able to read your direct messages (DMs). Determining if this setting is enabled is the first step in keeping your DMs secret.

- Once signed into Slack in a web browser, go to **slack.com/account/team** > click on **Retention Exports** > scroll down to **What data can my admins access** > if it only says public data can be exported, your DMs are safe from your supervisors.

- If admins have access to your direct messages, the message will read like this: **Workplace Owners can export messages and files from public channels**. Workspace Owners can also export messages and files from private channels and direct messages. If you see that message, it is recommended to set your direct messages to expire instead of just leaving them around. To do that, select the gear icon in the upper right corner when you're in a direct message, then select **edit message retention** > click **Next** > tap on **Use custom retention settings for this conversation** > Set it to **one day**, then select **Save**.

Customise message retention

By default, Slack will retain all messages and files for the lifetime of your workspace. If you like, you can have them deleted after a set amount of time.

- **Standard and Plus subscriptions:** from your desktop, click your workspace name in the top left > select **Settings & administration** from the menu > click **Workspace settings** from the menu > click the **Settings** tab at the top of the page > next to **Message retention & deletion**, click **Expand** > select your preferred retention settings > click **Save** > tick the box next to **Yes, apply these new settings** > click **Confirm settings**.

- **Enterprise Grid subscription:** From your desktop, click your workspace name in the top left > select **Settings & administration** from the menu, then click **Workspace settings** > from the **Settings** tab, find **Message retention & deletion** > click **Expand** and select your preferred retention settings > click **Save** > tick the box next to **Yes**, apply these new settings > click **Confirm settings**.

Convert a channel to private

- Only workspace owners, channel managers, and workspace admins can convert a channel to private, and they will need to be a member of the channel to do so. The #general channel cannot be converted to a private channel. Shared channels will only be converted in the workspace that makes the change. Files shared within the channel will not become private.

- **From your desktop:** open the channel that you want to make private > click on the channel name in the conversation header > select **Settings** tab > Choose **Change to a private channel** > click **Change to private** to confirm. A message will post in the channel to let members know that it's been converted.

- It's not possible to convert a channel to private from the Slack iOS or Android app.

Remove users in channels

- Open channel > click on the cluster of profile photos in the top right > find the person that you'd like to remove > next to their name click **remove** > click **remove to confirm**.

SNAPCHAT

Set up Two-Factor Authentication

- Go to your profile and click on the settings button > select **Two-Factor Authentication** > tap **Continue** to finish setting it up > choose **text message** or an **authenticator app** to receive your login codes.

Change your privacy settings

By default, only friends you've added on Snapchat can contact you directly or view your Story.

- Go to your profile and click on the setting button > scroll down to the **Privacy Controls** section and tap the options below. Once changes have been made, tap the **back** button to save your choice.

  – **Who Can Contact Me:** choose who can contact you directly with Snaps, Chats, calls, etc. If you choose **Everyone** for **Who Can Contact Me**, even users you haven't added will be able to send you Snaps and Chats.
  – **Who Can View My Story:** choose who can view your Story. Tap **Custom** if you'd like to block specific friends from seeing your Story.
  – **Who Can See My Location:** choose who can view your location on the Snap Map. Your location won't be shared on the Map until you open it for the first time.
  – **Who Can See Me In Quick Add:** Choose who can see you in Quick Add, a feature that appears around Snapchat which makes it easier to add friends.

Even if you choose **My Friends**, anyone you're in a group with will be able to communicate with you in Group Chat. To see who's in a group before you join it, just press and hold the name of the group in the Chat screen.

If you choose **My Friends**, you won't see Snaps sent to you by non-friends – you'll just get a notification that they added you as a friend. If you add them back, you'll be able to see Snaps they've sent you.

If you post a Snap to your Story, and then change your settings so only friends can see your Story, others may still be able to see the Snaps you posted before the change.

Set up My Eyes Only for the first time

- Swipe up from the Camera Screen to open **Memories** > press and hold on a Snap and tap **My Eyes Only** > select **Quick Setup** > create a passcode > this will be your new passcode and is the only way to access **My Eyes Only**. If you don't want to use a 4-digit passcode, you can set a passphrase of letters and numbers and select **Use Passphrase** at the bottom instead > read the information, and if you agree, tap **Continue** > once done, tap **Finish**.

Move snaps from Memories to My Eyes Only

My Eyes Only is for Snaps that you want to keep extra private. You can move Snaps and Stories in your **Memories** to **My Eyes Only**, then you can only see them after you enter your passcode.

- Swipe up from the Camera screen to open **Memories** > tap the checkmark option in the top right corner of your memories > select the snaps and stories you want to move to **My Eyes Only** > tap the lock icon at the bottom of the screen > tap **Move** > you may be prompted to enter your passcode.

Switch off location settings

- To turn off your location, go to your phone settings > scroll down and tap on **Privacy & Security** > click on **Location Services** > scroll down to **Snapchat** > choose to **never share**. If Snapchat does not appear on this list, go to the map function in the Snapchat app. This will prompt you to choose whether to share your location > choose to **never share.**

- You can enable the **Ghost Mode**. With this setting enabled, your friends won't be able to see your location on the map: go to your profile and click on the setting button > scroll down and click on **Who Can See My Location** > switch on **Ghost Mode**. You can choose to have it on for **3 hours**, **24 hours**, or just until you turn it off yourself.

- You can also share your location with specific friends only: in **Who Can See My Location**, disable **Ghost Mode** and decide who can see you on the map and choose between **My Friends**, **My Friends, Except...** and **Only These Friends**.

- You can also prevent location requests altogether: in **Who Can See My Location**, toggle off **Allow friends to request my location**.

SNAPCHAT

Remove a friend from friend list

- Swipe right to go to the Chat screen > tap and hold on a friend's name > tap **More** > tap **Remove Friend**.

Block a friend

When you block a friend, they won't be able to view your Story or Charms, or send you Snaps or Chats. Additionally, these users will not be able to contact you or send you unwanted add requests on Snapchat.

- Swipe right to go to the Chat screen > tap and hold on a friend's name > tap **More** > tap **Block**.

Manage your contacts

- Go to your profile and click on the **Settings** button > scroll down to **Additional Services** > tap on **Manage** > click on **Contacts** > disable **Sync Contacts**.

Manage your advert preferences

- **iOS:** Go to your profile and click on the setting button > scroll down to **Additional Services** > tap on **Manage** > select **Advert Preferences** > disable **Audience-Based**, **Activity-Based** and **Third-Party Ad Networks**.

- **Android:** Go to your profile and click on the setting button > scroll down to **Features** and tap **Ads** > select **Advert Preferences** > disable **Audience-Based**, **Activity-Based** and **Third-Party Ad Networks**.

Manage your lifestyle categories

- **iOS:** Go to your profile and click on the setting button > scroll down to **Additional Services** and tap **Manage** > go to **Lifestyle & Interests** > choose a **Lifestyle Category** to turn it **on** or **off**. Additionally, while on the **Lifestyle & Interests** page, scroll down and tap **Clear Content Interests Tags**, and choose an **Ad Topic** to turn it **on** or **off**.

- **Android:** Go to your profile and click on the **Settings** button > scroll down to **Features** and tap **Ads** > go to **Lifestyle & Interests** > choose a **Lifestyle Category** to turn it **on** or **off**. Additionally, while on the Lifestyle & Interests page, scroll down and tap **Clear Content Interests Tags**, and choose an **Ad Topic** to turn it **on** or **off**.

Access your data

- Log in to your account on accounts.snapchat.com > click on **My data** > click **Submit request** at the bottom of the page > if you have verified an email address with Snapchat, an email will be sent to you with a link once your data is ready to download. Ensure you do not share this link with anyone > follow the link in your email to download your data > click the link to download your data.

NETFLIX

Set maturity levels for profiles

On the Viewing Restrictions page, there are various content age ratings adapted to what you'd like for your child: TV-Y (6 and under); TV-Y7 (7 and younger); TV-G/G (general audience); TV-PG/PG (parental guidance); etc. These restrictions are set according to the MPAA and TV rating systems.

- From a web browser, go to your Account page > open the **Profile & Parental Controls** settings for the profile you want to manage > change the **Viewing Restrictions** setting > enter your Netflix password > set the maturity rating level for the TV shows and movies you want to allow in that profile > select **Save**. TV shows and movies above the selected maturity level will be removed from the profile.

Restrict access to a profile with a profile lock PIN (this is not two-factor authentication which Netflix doesn't offer)

- Sign into Netflix with a web browser and go to your Account page > open the **Profile & Parental Control** settings for the profile you wish to lock > change the profile lock setting > enter your Netflix account password > check the box to require a PIN to access the selected profile > to remove the PIN requirement, uncheck the box > enter four numbers to create your profile lock PIN > select **submit**.

Once your PIN is set, Netflix will ask for it whenever that profile is chosen at the welcome screen. This will happen on all devices, including TVs. Note that Netflix will not ask for a PIN if your profile is the only one that exists on the account.

Any profile on your Netflix account can be given its own PIN, but only the account holder can set them up. The Netflix account owner always has the power to disable the PIN and profile lock for any profile.

Set up your phone number for password recovery

Netflix can send you a text message with a code to recover your account if you forget your password.

- First, you need to make sure you have a correct and verified phone number added to your account. From a web browser, go to your Account page > go to the **Membership & Billing** section and select **Add phone number** or **Change phone number** > select your country > enter your phone number > enter your account password.

Hide titles from viewing history

When hiding titles from your viewing history, they won't appear in Netflix as a TV show or movie you've watched. They won't be used to make recommendations to you, unless you watch them again. They'll also be removed from the Continue Watching row.

- Sign into Netflix with a web browser and go to your Account page > open **Profile & Parental Controls** for the profile you want to update > open **Viewing Activity** for that profile > on the Activity page, click the **hide** icon next to the episode or title you want to hide. If you hide an episode, you'll see the option to hide the entire series > to hide all of your viewing history, select the **Hide all** option at the bottom of the page and **confirm**. It can take up to 24 hours for a hidden title to be removed from all your devices. Titles can't be hidden if the Activity page is reached from a Netflix Kids profile.

Turn autoplay previews off

To prevent TV shows and movies from quickly sampling, you can set Netflix to stop automatic previews.

- From a web browser, go to your Account page > open the **Profile & Parental Controls** settings for the profile you want to use > select **Playback settings** > check **Autoplay previews** while browsing on all devices > to stop autoplaying previews, uncheck the box > select **Save**.

Sign out of all your devices

To remove unauthorized access to your Netflix account, it is recommended to sign out of all devices on your account.

- Sign into Netflix with a web browser and go to your Account page > under **Settings**, select **Sign out of all devices** > you'll be asked to confirm your choice > finally, click **Sign out**. It can take up to 8 hours to sign out of all devices. After the devices have been removed, we recommend that you change your password.

TWITTER

Enable Two-factor Authentication

- When on the main page, tap on your Profile on the top left and scroll down to **Settings and privacy**. Go to **Security and account access** and then tap **Security**. Go to **Two-factor authentication**. Select the method of second authentication. You can choose between **Text message**, **Authentication app** and **Security key**. Follow the prompts on screen to complete the process.

Protect your account

- Tap on your Profile on the top left and scroll down to **Settings and privacy**. Go to **Security and account access** and then tap **Security**. Enable **Password reset protect (to the right)**. With this setting enabled, you will need to confirm your email address or phone number to reset your Twitter password.

Protect your Tweets

- Tap on your Profile picture on the top left and scroll down to **Settings** and **privacy**. Go to **Privacy and safety** and tap **Audience and tagging**. Toggle on **Protect your Tweets** (to the right). This will ensure only people who follow you will see your Tweets.

Disable photo tagging

- Tap on your **Profile picture** on the top left and scroll down to **Settings and privacy**. Go to **Privacy and safety** and tap **Audience and tagging**. Go to **Photo tagging** and toggle off the setting (to the left). If you wish to have the setting on, select **Only people you follow can tag you** instead of **Anyone can tag you**.

Control who can find you

- Tap on your Profile and scroll down to **Settings and privacy**. Go to **Privacy and safety** and scroll down to **Discoverability and contacts**. Toggle off **Let others find you by your email** and **Let others find you by your phone**. If you wish, you can also disable **Sync address book contacts** in this section.

Hide your location

- Tap on your Profile and scroll down to **Settings and privacy**. Go to **Privacy and safety** and scroll down to **Location information**. Tap on **Precise location** and disable the setting. In the **Location information** section, you can also disable the **Personalise based on places you've been** setting.

Control your data

- Tap on your Profile picture on the top left and scroll down to **Settings and privacy**. Go to **Privacy and safety** and scroll down to the **Data sharing and Off-Twitter activity**. Turn off the **Personalised ads** setting in **Ads preferences**, turn off **Personalise based on your inferred identity** and turn off **Allow additional information sharing with business partners**.

Schillings

12 Arthur Street
London
EC4R 9AB
T: +44 (0)20 7034 9000

One World Trade Center
Suite 8500
New York, NY 10007
T: +1 (212) 220 5761

Schillings International (USA) LLP is a registered limited liability partnership organised and existing under the laws of the State of Delaware, United States of America, whose principal place of business is at One World Trade Center, Suite 8500, New York, NY 10007. Our New York based attorneys are registered as a foreign legal consultant in the State of New York.

SCHILLINGS

schillingspartners.com