A GUIDE TO

Reducing Online Abuse and Harassment

This booklet has been created using a variety of online resources and professional expertise to help you secure you and your family's online accounts

harbour
working for safer communities

THE BUSINESS RESILIENCE CENTRE FOR THE NORTH EAST

NERSOU | Protecting communities from organised crime

Introduction

Sometimes online abuse can be more harmful than physical abuse and it can seem like there is no escaping it. Now that technology is an essential part of our daily lives, we often have no choice but to use online services to work or keep in touch with family and friends. Although it may seem difficult, the good news is that you can use these services safely. By making small changes to your account settings, you can drastically reduce your digital footprint (the amount of personal information about you or your family which is online for unauthorised others to see). This booklet contains easy to follow, step-by-step guides of how to secure key accounts, alongside digital services and children's accounts and devices.

Lots of people have given their expertise to this, including North East Business Resilience Centre (NEBRC) ethical hackers, students studying cyber security at Northumbria and Sheffield Hallam Universities, the North East Special Operations Units cyber team, Cleveland Police's cyber team, Durham Constabulary's safeguarding and cyber teams and Harbour, an independent charity which helps support victims of domestic abuse.

The NEBRC is a non-for-profit centre, which brings together policing, academia and private sector businesses to help keep our communities safe from online attacks and harm. The information and guidance contained in this booklet is one example of how our centre is reinvesting its profits back into our communities for the public good.

We encourage people to use technology and online services, they are great enablers of communication and have improved the way we live our lives. We know that securing this technology can sometimes seem really complicated, but you only need to make small changes, and hopefully this guide can help you make sense of them.

Remember if you ever feel unsafe or at risk of harm, please contact the police, and we hope this booklet helps you keep you and your family that little bit safer.

Regards,

Rebecca

Superintendent Rebecca Chapman
Director of the North East Business Resilience Centre

Contents

The following actionable guidance can be implemented to make individuals safer from online stalking and harassment. It does not guarantee that such abuse will be stopped and there are pro's and con's to implementing this guidance. It is for each individual concerned to consider their circumstances and implement what they feel is appropriate for them. Remember to contact the police immediately if you feel unsafe or at risk of harm.

Password

RECOMMENDATIONS

Tips and Tricks

These recommendations make passwords more difficult to guess and compromise

Prioritise length over complexity

Create your password from 3 random words

Include symbols and numbers

Do not reuse passwords or pins!

Security

To keep your password secure, keep in mind:

- Ex-partners may know your passwords or the sensitive information used for security questions, so you should change them
- A good rule is that your password should not be easily guessed by someone who knows you

Poor passwords include:

- Maiden names
- Names of pets
- Favourite things - e.g. bands, books, films
- Place of birth
- Favourite teams - e.g. football, rugby

This is all information your friends and family may know, and others may be able to discover on your profiles

Password Managers

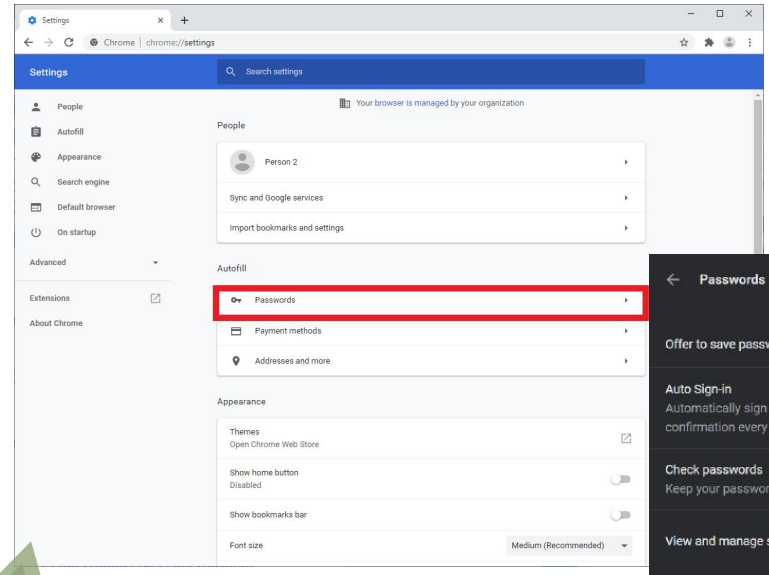
- A password manager is a programme that is designed to create and store strong, unique passwords for you
- It can be locked with a password or two-factor/multi-factor authentication for increased security
- It creates complex passwords using factors you can personalise
- There are many varieties - some free and some that require payment
- They help reduce password reuse by creating unique passwords for you

Biometric Passwords

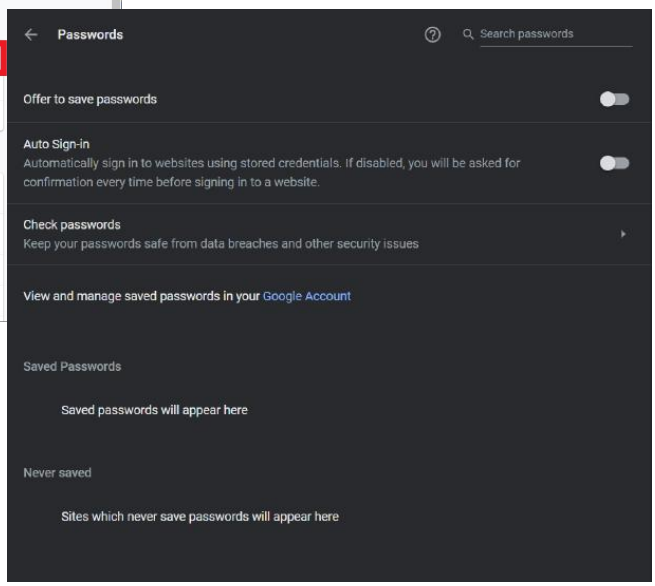
- A biometric password is one that requires a physical characteristic of the person associated with the device - e.g. fingerprint, facial recognition
- Enabling biometrics on your personal devices can be beneficial for security and make logging in quicker and easier

Remember:

- Relying on biometrics alone could weaken security as your fingerprint or face scan could be taken by somebody who can access your device while you sleep
- It is always best to have multiple layers of security, the more you have the harder it is to get into your device or account - combine biometrics with passwords and pins if possible, this is call multi-factor authentication (MFA)



Make sure to remove your passwords from old devices including those stored in browsers, password managers, settings etc.



Password settings can be found in the auto-fill section of your browser 'Settings' menu

These can be removed and placed into your new password managers before deletion

Pins and Devices

- All devices should have pins on them to prevent unauthorised access
- Pins should be unique - avoid common ideas such as bank pins, date of birth and parts of phone numbers
- Pattern locks can also be weak as smudges on the screen from their input can give away the code

Passwords on Voicemail and Messaging Apps

Voicemail services and some popular messaging apps (e.g. Whatsapp, Facebook Messenger) can be locked behind a second password - this is recommended in case the parent device is compromised

For voicemails the process is specific to each provider and can be found on your providers network

- Remember, lots of celebrities had their voice messages hacked by not password protecting their answer phone messages

Changing Passwords: Order of Importance

This order will be very different for each individual but keep in mind that some accounts are more important to keep secure than others

One possible order is:

1. Emails & password managers
2. Banking
3. Maps & tracking
4. Online ordering platforms
5. Social media
6. Holiday & hotel apps
7. Phone contracts

Two-Factor AUTHENTICATION

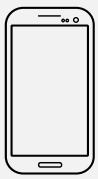
What is two-factor authentication?

Two-factor authentication (2FA) is used to improve account security. Often it takes the form of a code that comes to your phone as a text which you then input into your account (similar to a password) or a pop-up asking you to verify that the person attempting to log in is you

Why should you use it?

In the event your password is compromised, I it will alert you to any login attempt. For example, if someone attempts to log into your account you can deny them access by selecting 'no' on a verification pop-up or through them not having the code that you will receive. This keeps your account secure and gives you time to change the password

The most common type of 2FA is a 6-digit code sent to you as a text



2FA can be enabled on the majority of online services - from social media and emails, to online shops and PayPal

2FA is completely free and can be set up quickly and easily

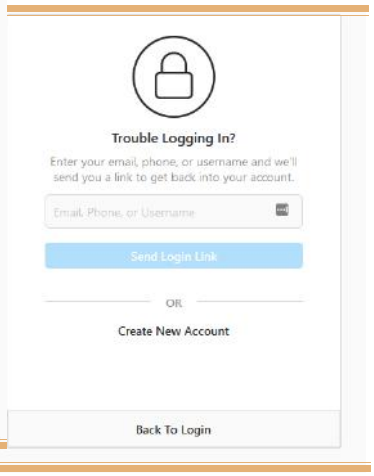
The majority of social media hacking cases reported to the police would have been prevented if 2FA had been enabled

The majority of services allow you to set up two-factor authentication in a similar way: often the option to turn it on can be found in the Settings menu, potentially under the headline 'Security'. Some services will ask if you want to set it up when you make the account

Recovering Your Instagram Account

1

Reset

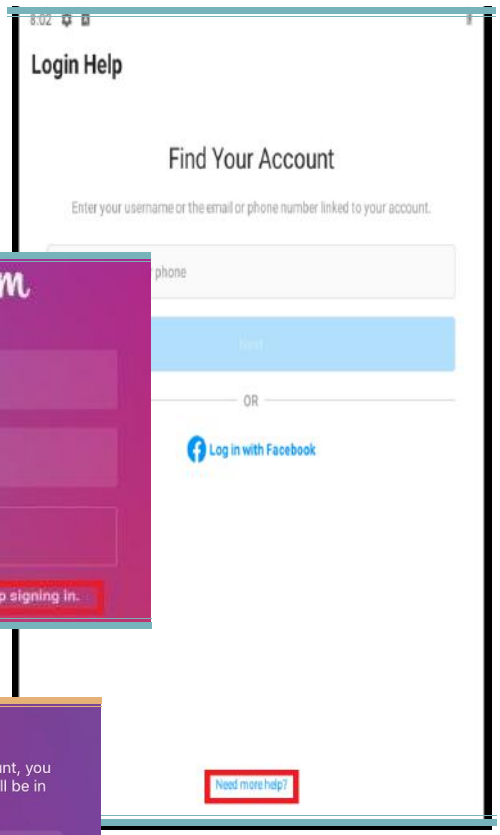


If you're unable to access your Instagram account then it may have been hacked - this makes it easier for someone to impersonate you

BE AWARE : if your account has been hacked then your username may have been changed

Password Reset

If you have noticed suspicious or unusual activity on your account or you are unable to access your account, the first thing to do is reset your password. This can be done by clicking 'Forgot password?' on the login page, then following the onscreen instructions or 'Create a New Account' if you want



2

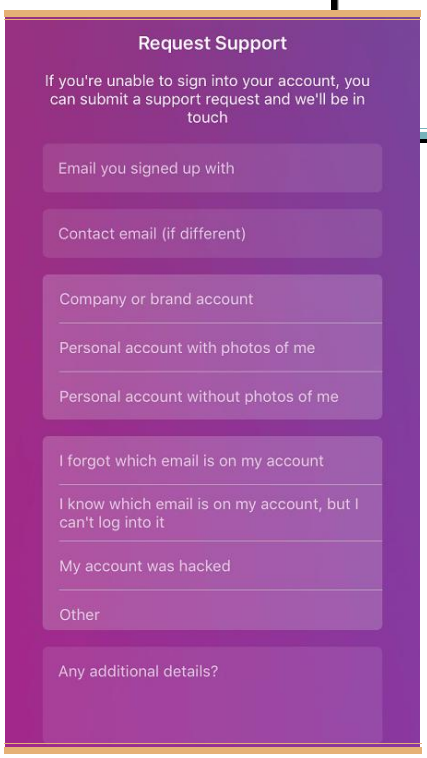
Help

Extra Help

For extra help click 'Get Help Logging In' on the login screen, then enter a username, email or phone number when prompted, finally click 'Need More Help?'

3

How



Request Support Form

Selecting 'Need more help?' will take you to the 'Request Support' form, enter your relevant email address, then select the appropriate account type and reason for support. You can then enter additional details that you think may help Instagram resolve the problem , before clicking the button at the bottom to send the form. After this you should receive an email to the address you entered

4

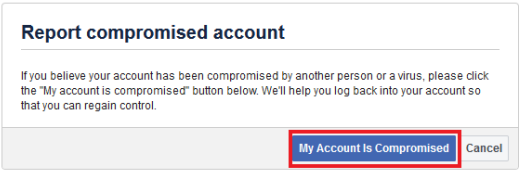
Control

Regaining Control

The email you receive will ask you to send a photo of yourself attached to an email, a hand-written note containing a code that Instagram will give you, your full name and the account username

Recovering Your Facebook Account

If you're unable to access your Facebook account then it may have been hacked - this makes it easier for someone to impersonate you

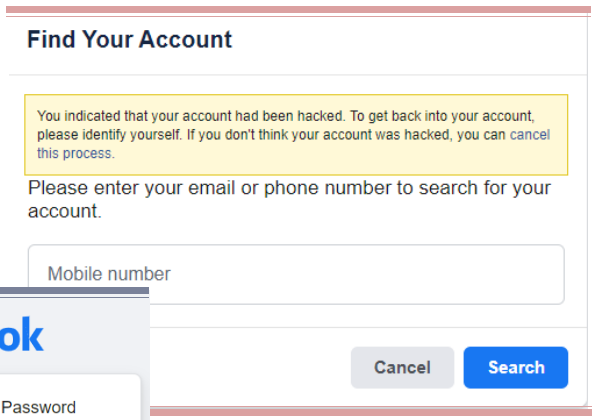


1

Recovery

Recover Your Account

If you think that your Facebook account has been hacked, type https://facebook.com/hacked into your search engine. Once this has loaded, clicking 'My Account is Compromised' will take you through steps to recover your account



2

Find

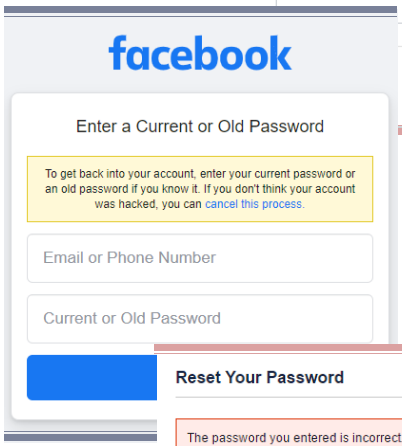
Find Your Account

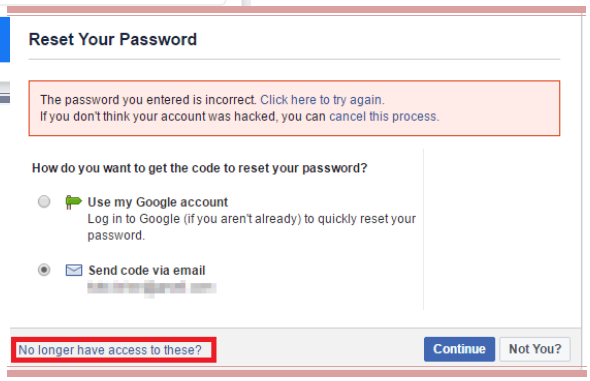
You will then be taken to a new page and asked to enter your phone number or email address that is connected to the account

3

How

How To Reset



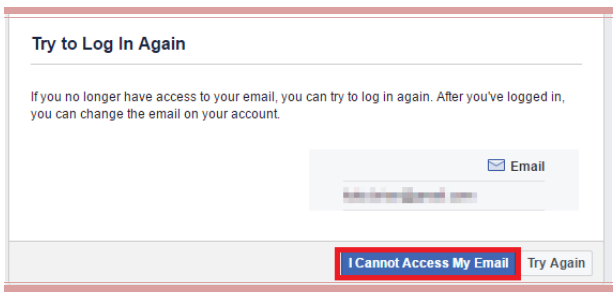


Next you will need to enter a current or old password with your phone number or email address, you can then choose how you would like to reset your password

4

Email

Compromised Email Account



Inputting an email address will send an email to that account containing a link to change your password - if your account has been hacked then the connected email address may also be compromised - to avoid alerting the hacker, use a different email address by clicking 'No longer have access to these?' and then 'I Cannot Access My Email' before following the onscreen instructions

Recovering Your Twitter Account

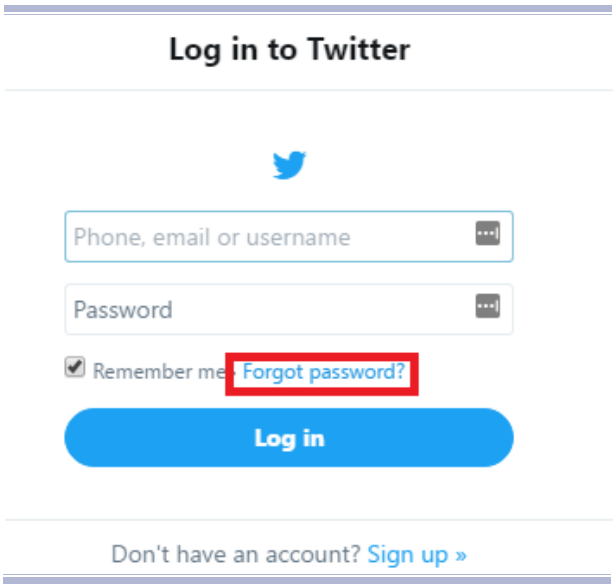
If you're unable to access your Twitter account then it may have been hacked - this makes it easier for someone to impersonate you

1

Reset

Password Reset

If you have noticed suspicious or unusual activity on your account or you are unable to access your account, the first thing to do is reset your password

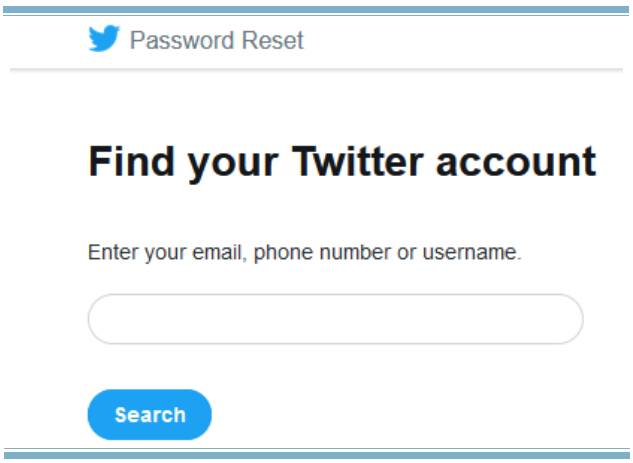


2

Find

Find Your Account

Twitter will ask for you to enter your email, phone number or username to find your account

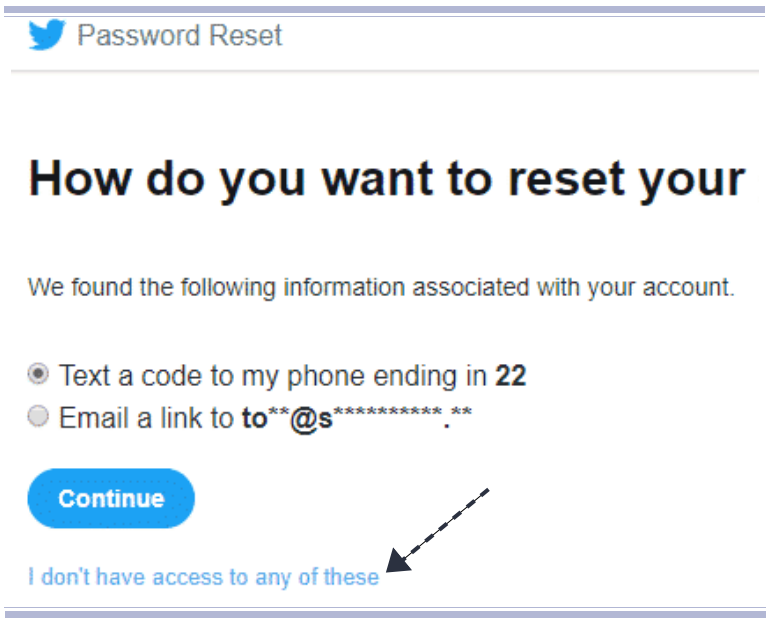


3

How

How To Reset

You will be asked how you would like to reset your password
Once you have picked a method, Twitter will contact you via it to give you steps to reset your password
If you do not have access to any of the given choices, click 'I don't have access to any of these' underneath the 'Continue' button



SECURING YOUR BROWSER

Safari

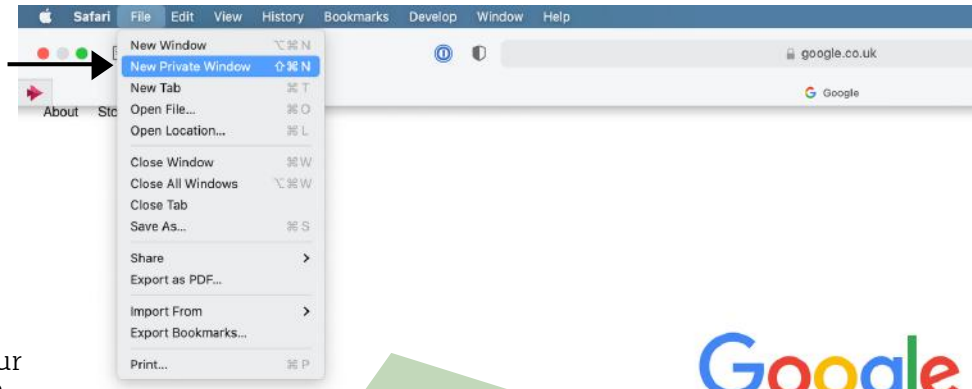
Whilst there is no guarantee that the steps below will provide maximum security, they are intended to help in making your personal information more difficult for others to access, enabling you to browse the internet more safely and securely

Private Browsing

Browsing in a private window (also known as 'incognito mode') offers additional privacy to that in a normal window

Incognito Mode will not remove sites that have been bookmarked during its use or hide any downloaded files

To turn on Incognito Mode:
1. Open Safari and go to 'File' in the top left hand corner of the screen
2. In the dropdown menu select 'New Private Window'



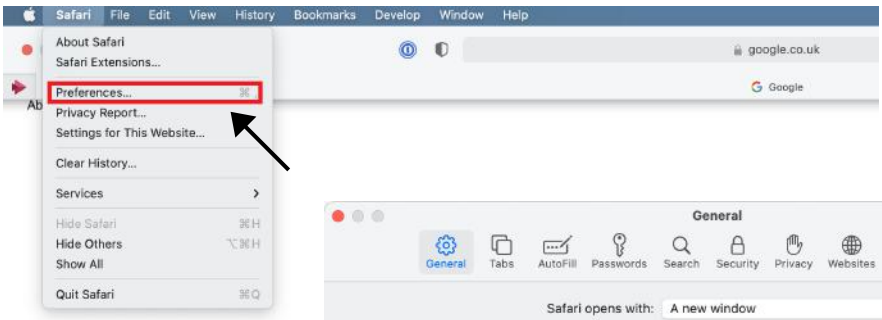
Whilst using Incognito Mode will increase your privacy, it is advised that you further secure your browser using the following steps

Incognito Mode will delete your search history and cookies when you close the browser

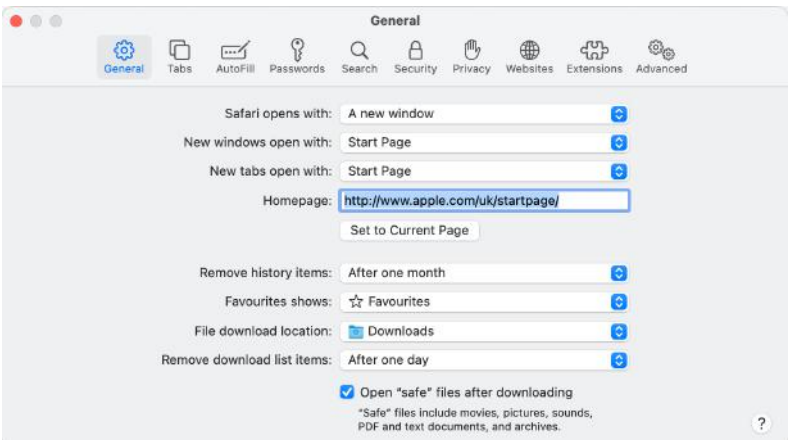
Changing Your Settings

You can adjust the settings associated with Safari to improve your security and privacy

To change your settings:
1. Click on 'Safari' in the top left hand corner
2. Select 'Preferences...' in the dropdown menu

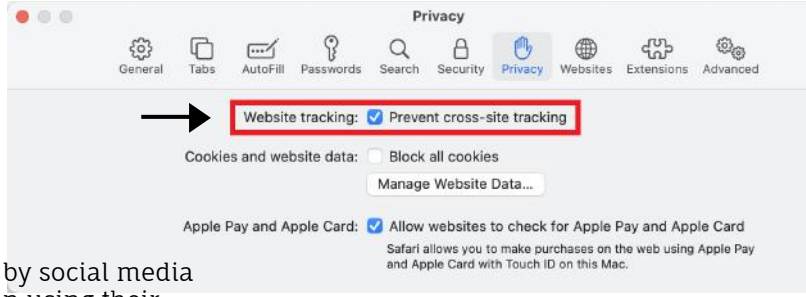


The General Settings menu will appear for you to adjust accordingly



Privacy

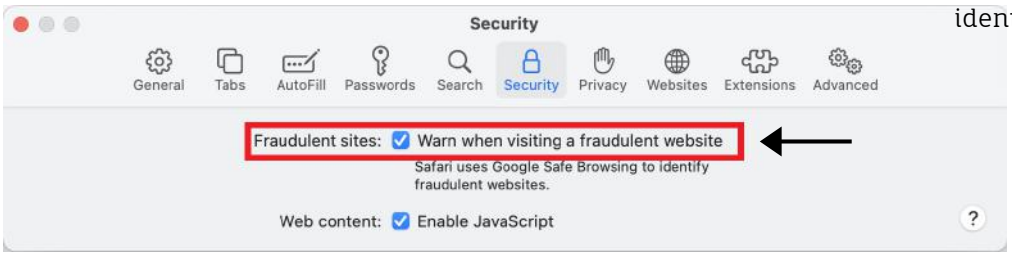
In the 'Privacy' section, you can tick 'Website tracking: Prevent cross-site tracking' to prevent websites from tracking your browsing



'Cross-site tracking' is often used by social media to show you relevant adverts when using their site - these are shown to you based on what sites you use when this type of tracking is enabled

Security

When browsing the web you may unknowingly visit sites that are fraudulent - safari can help identify and warn you of these

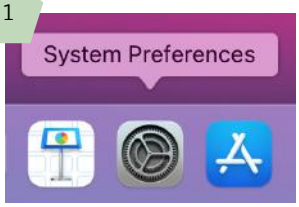


To turn this on:
1. Go to the 'Security' tab in Settings
2. Tick 'Fraudulent sites: Warn when visiting a fraudulent website'

Updates

Like software and apps, keeping your browser up to date will improve your security by protecting your private information from being accessed by unwanted people

1

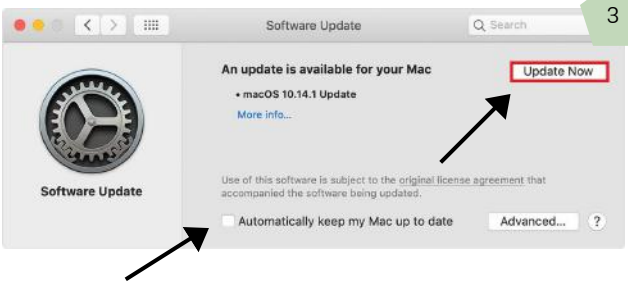


Safari is updated when you complete a system update on your device

2

To update Safari:
1. Access 'System Preferences'
2. Select 'Software Update'
3. If you need to do an update, click the 'Update Now' button

3



To become more efficient with software updates, tick 'Automatically keep my Mac up to date'

SECURING YOUR BROWSER

Firefox

Whilst there is no guarantee that the steps below will provide maximum security, they are intended to help in making your personal information more difficult for others to access, enabling you to browse the internet more safely and securely

Private Browsing

Browsing in a private window (also known as 'incognito mode') offers additional privacy to that in a normal window

Incognito Mode will not remove sites that have been bookmarked during its use or hide any downloaded files

Incognito Mode will delete your search history and cookies when you close the browser

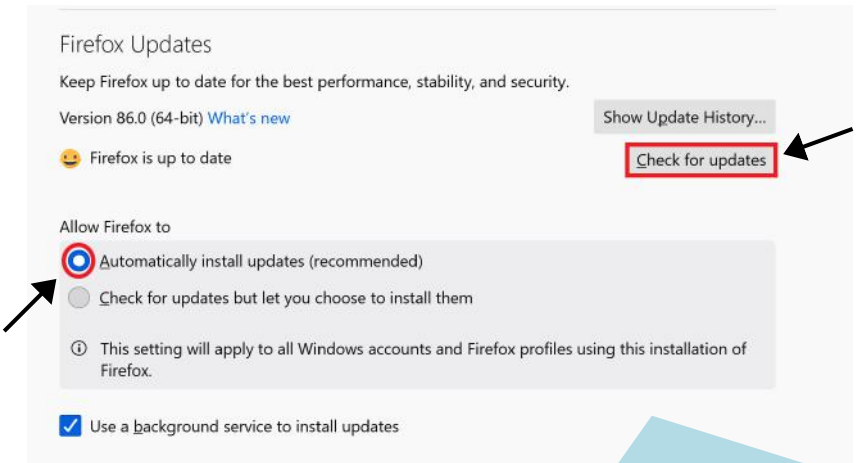
To turn on Incognito Mode:
1. Open Firefox
2. Click on the three horizontal lines on the right hand side of the address bar
3. Select 'New Private Window'

Whilst using Incognito Mode will increase your privacy, it is advised that you further secure your browser using the following steps

Updates

Like software and apps, keeping your browser up to date will improve your security by protecting your private information from being accessed by unwanted people

To check if Firefox is up-to-date:
1. Access 'Options' as to the left
2. Select 'Firefox Updates' in the 'Options' menu
3. Click the 'Check for Updates' button

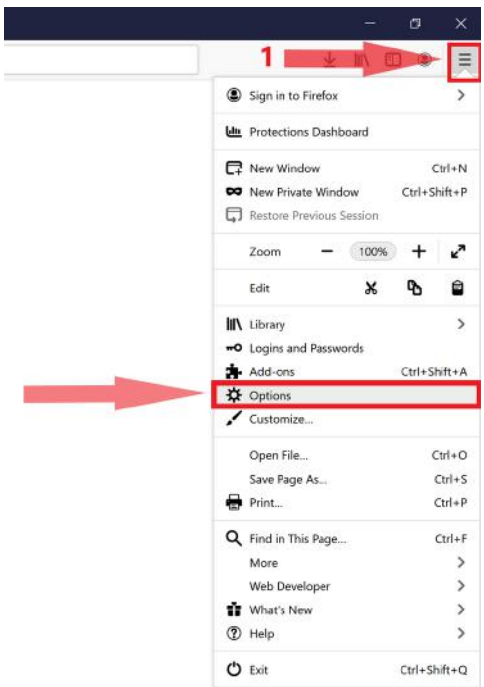


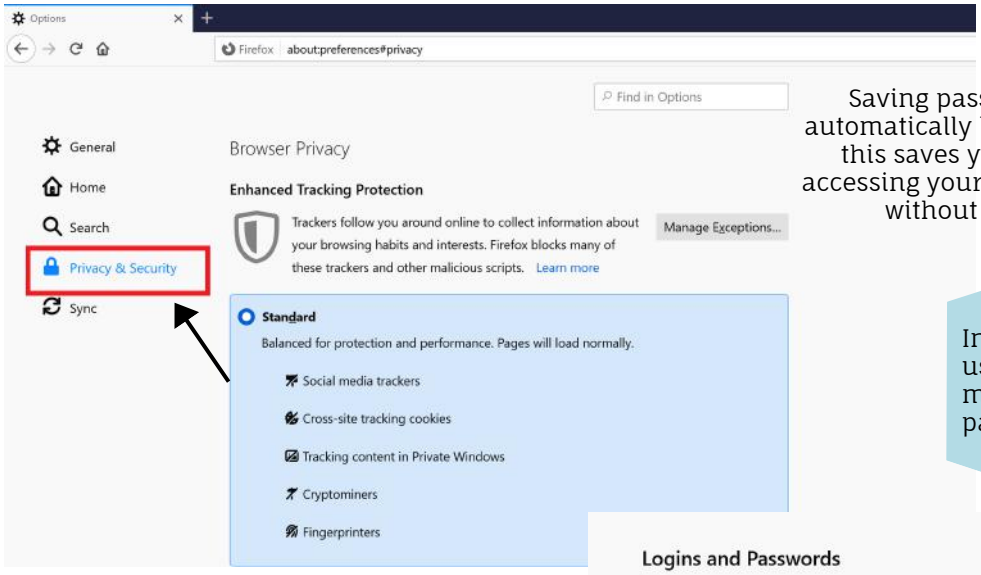
To become more efficient with updates, enable 'Automatically install updates (recommended)' by selecting the relevant circle on the left hand side

Changing Your Settings

You can adjust the settings associated with Firefox to improve your security and privacy

To change your settings:
1. Click on the three lines as before
2. Select 'Options'





Passwords

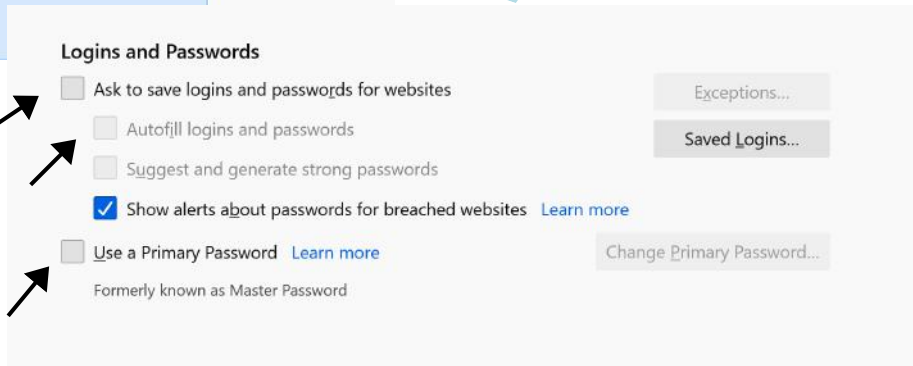
Saving passwords in your browser allows it to automatically log you in when you visit a site, whilst this saves you time, it also means that anyone accessing your computer can log in to your accounts without having to know your passwords

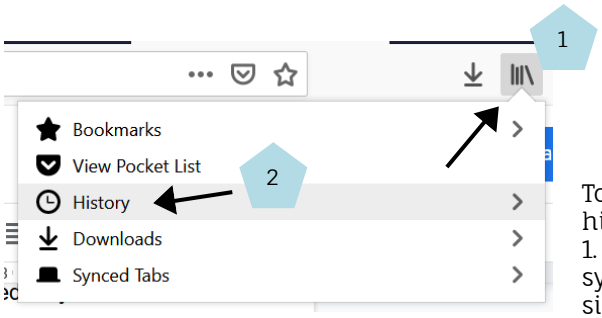
Increase your security by using a suitable password manager rather than saving passwords to your browser

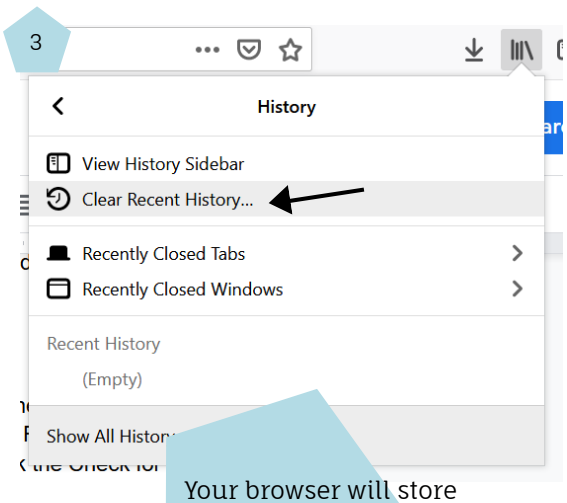
It is recommended that you access 'Privacy and Security' in the 'Options' menu, and turn the following settings off by unticking the boxes:

- Ask to save logins and passwords for websites
- Auto fill logins and passwords
- Use a primary password

Keep 'Show alerts about passwords for breached websites' on by ticking the box



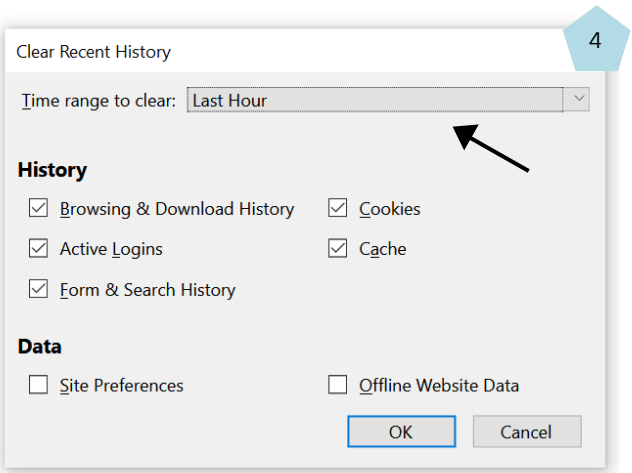




Browsing History

By accessing your 'History' somebody can see what websites you have been on and reload them - you can clear this to keep your browsing history private

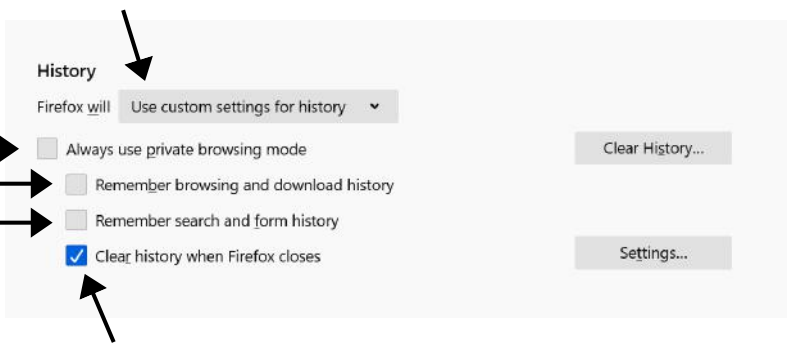
To clear your browsing history:
1. Click the four books symbol on the right hand side of the search bar
2. Select 'History'
3. Choose 'Clear Recent History'
4. Using the drop-down menu next to 'Time range to clear' you can choose how much of your browsing history you would like to delete



Your browser will store your browsing history until it is deleted

To have Firefox delete your history on closing the browser:
1. Access 'Privacy and Security' in the 'Options' menu
2. Scroll down the page to the 'History' section - here you can set how much you would like your browser to remember
3. Using the drop-down menu next to 'Firefox will', select 'Use custom settings for history'
4. Untick all of the boxes below this <u>except</u> 'Clear history when Firefox closes'

You can adjust settings to have Firefox clear your history when you close the browser



SECURING YOUR BROWSER

Google Chrome & Microsoft Edge

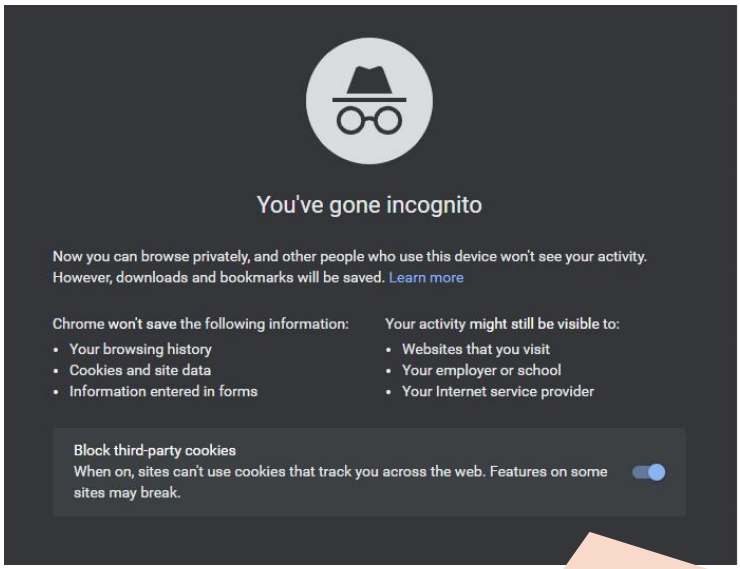
Google Chrome and Microsoft Edge are very similar and have the same options available in the 'Settings' menu

Whilst there is no guarantee that the steps below will provide maximum security, they are intended to help in making your personal information more difficult for others to access, enabling you to browse the internet more safely and securely

Private Browsing

Browsing in a private window (also known as 'incognito mode') offers additional privacy to that in a normal window

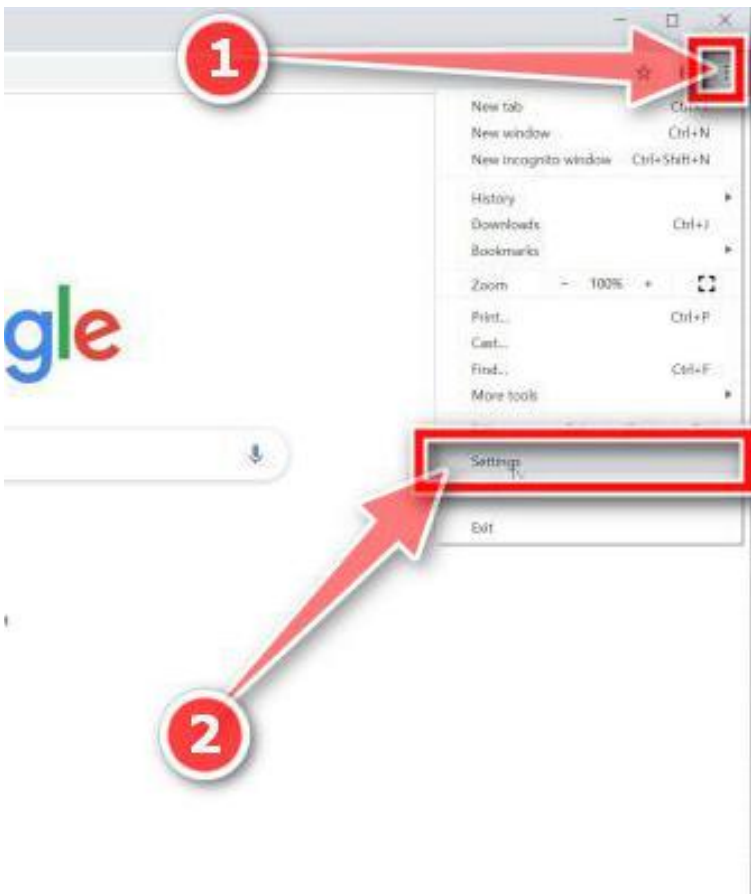
To turn on Incognito Mode:
1. Open your browser
2. Click on the three vertical dots on the right hand side of the address bar
3. Select 'New Incognito Window'



Incognito Mode will not remove sites that have been bookmarked during its use or hide any downloaded files

Whilst using Incognito Mode will increase your privacy, it is advised that you further secure your browser using the following steps

Incognito Mode will delete your search history and cookies when you close the browser



Changing Your Settings

You can adjust the settings associated with your browser to improve your security and privacy

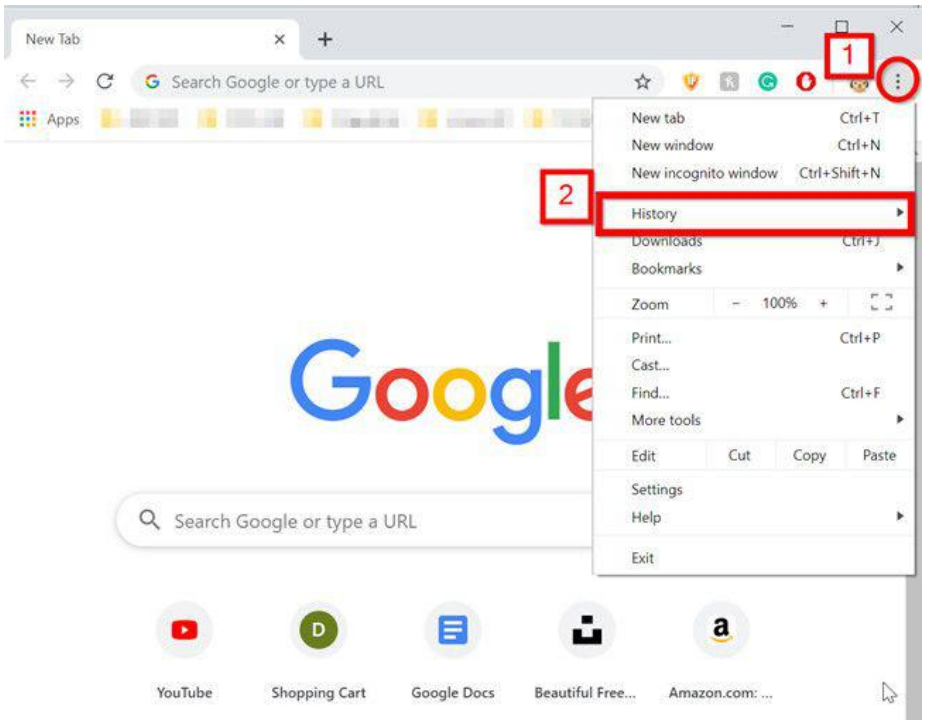
To change your settings:
1. Click on the three vertical dots as above
2. Choose 'Settings'

To check that your browser is up-to-date, click the same vertical dots and select 'Help' then find the 'About' section

Browsing History and Cookies

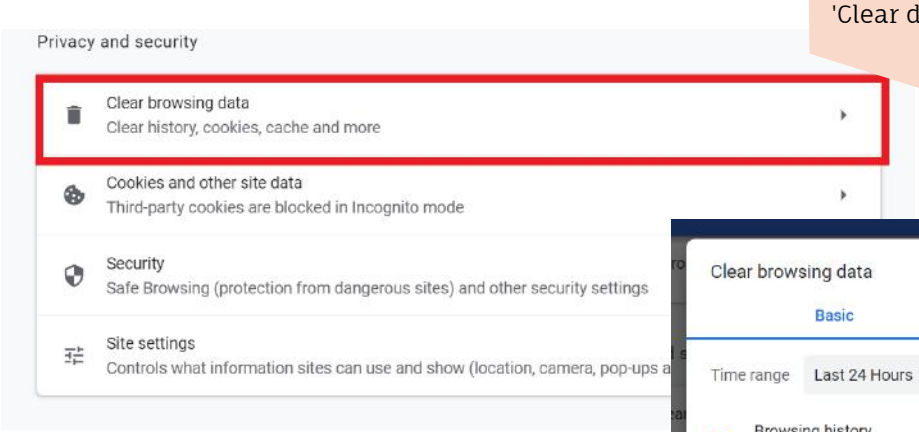
By accessing your 'History' somebody can see what websites you have been on and reload them - you can clear this to keep your browsing history private

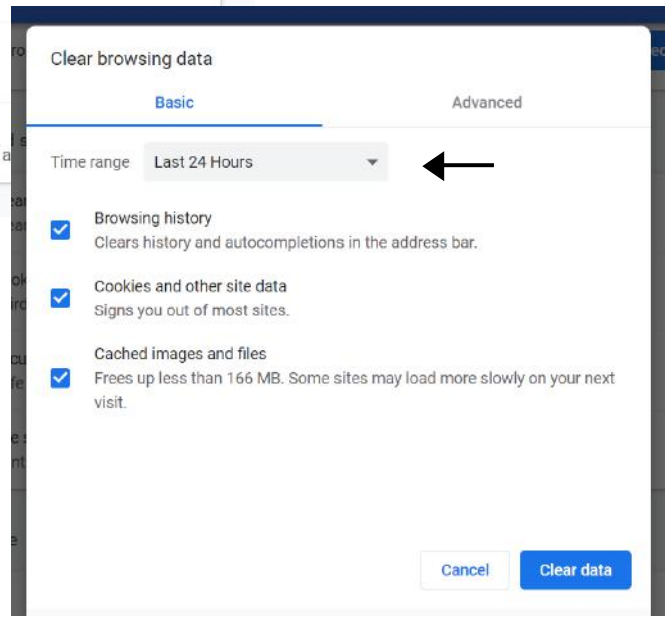
To see your browsing history:
1. Click the three vertical dots to the right of the address bar
2. Select 'History' in the drop-down menu - here you can view all stored, previously visited websites and reload them



To delete your browsing history:
1. Navigate to the browser 'Settings'
2. Find the 'Privacy and security' section
3. Click 'Clear browsing data'
4. In the window that appears you can choose how much of your browsing history to delete using the drop-down menu next to 'Time range'
5. Press the 'Clear data' button

You can also delete any saved cookies by ticking 'Cookies and other site data' before pressing 'Clear data'

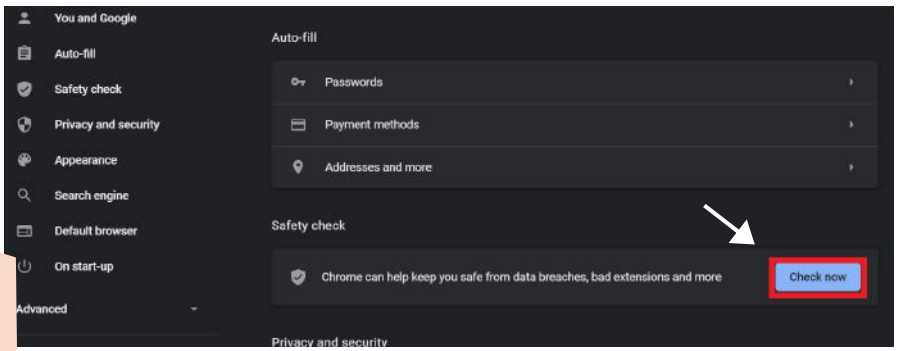




Perform a Safety Check

Like software and apps, keeping your browser up to date will improve your security by protecting your private information from being accessed by unwanted people

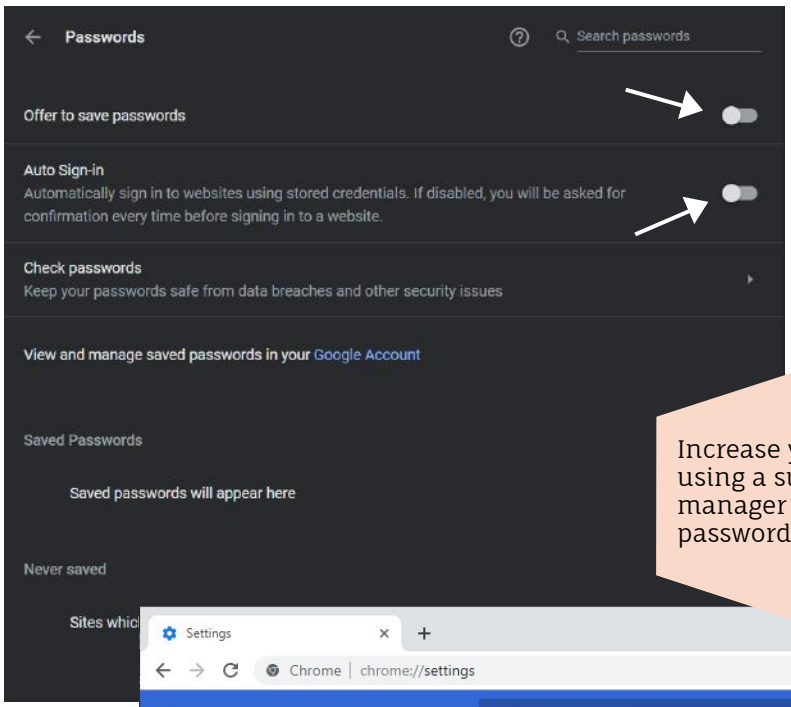
To do a quick safety check:
1. Access the 'Safety Check' section of your browser settings
2. Click the 'Check Now' button



A 'Safety Check' analyses your browser's security settings to highlight any potential weaknesses

Passwords

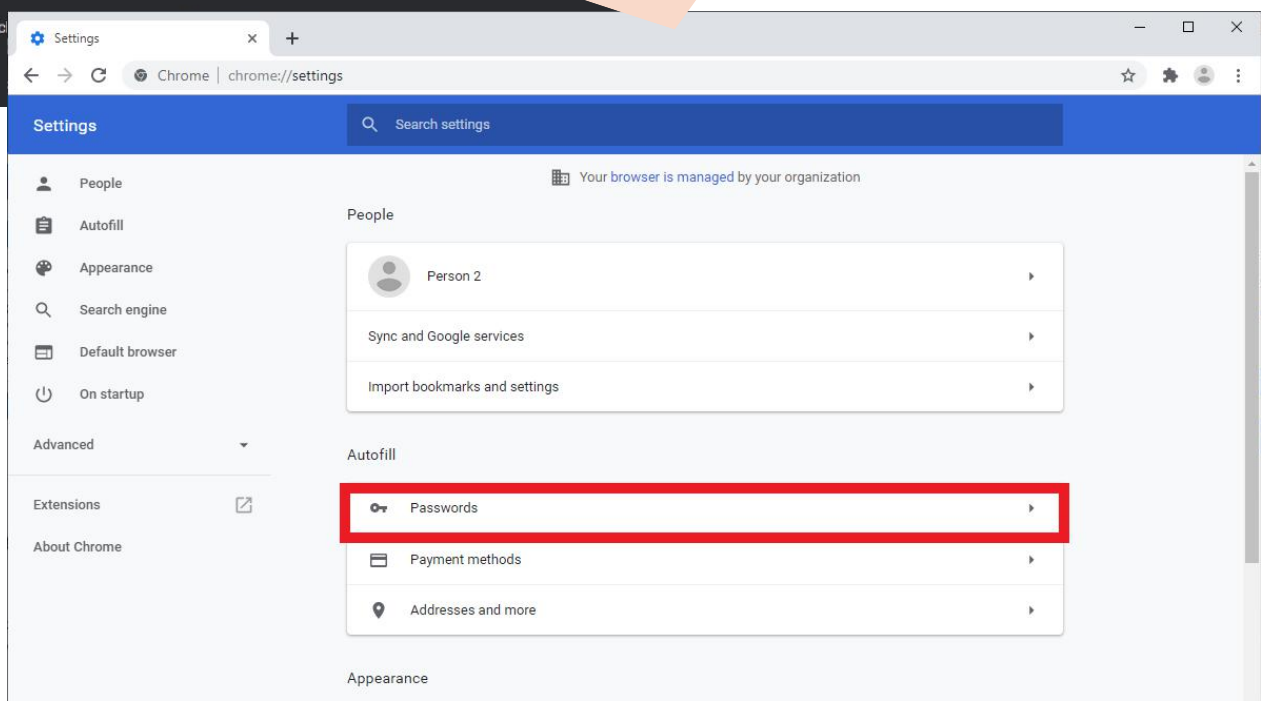
Saving passwords in your browser allows it to automatically log you in when you visit a site, whilst this saves you time, it also means that anyone accessing your computer can log in to your accounts without having to know your passwords



It is recommended that you access 'Passwords' in the 'Settings' menu and turn off the following:

- Offer to save password
- Auto sign-in

Increase your security by using a suitable password manager rather than saving passwords to your browser

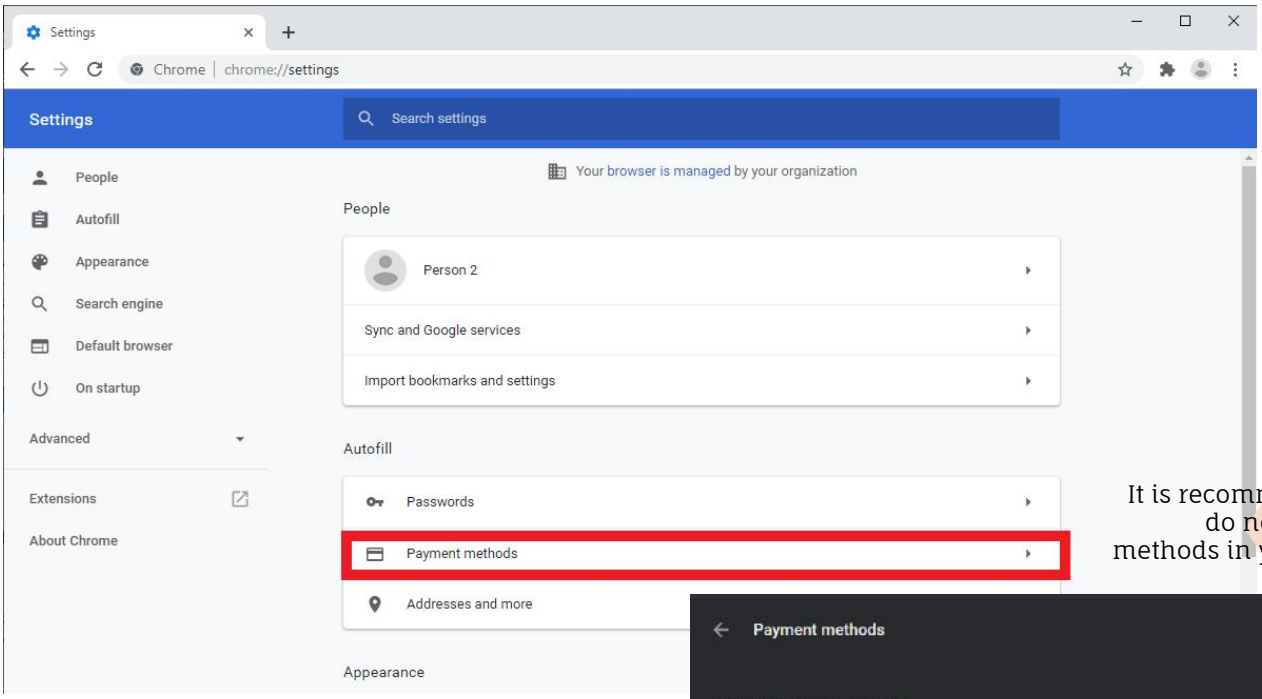


Payment Methods

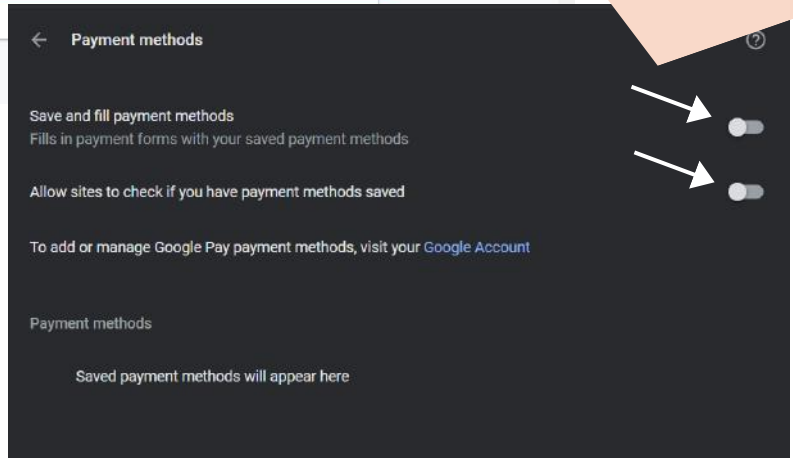
Saved payment methods can be used without your knowledge by anyone with access to your browser

It is advised that you go to the 'Auto-fill' section of your 'Settings' and turn off the following options:

- Save and fill payment methods
- Allow sites to check for stored methods



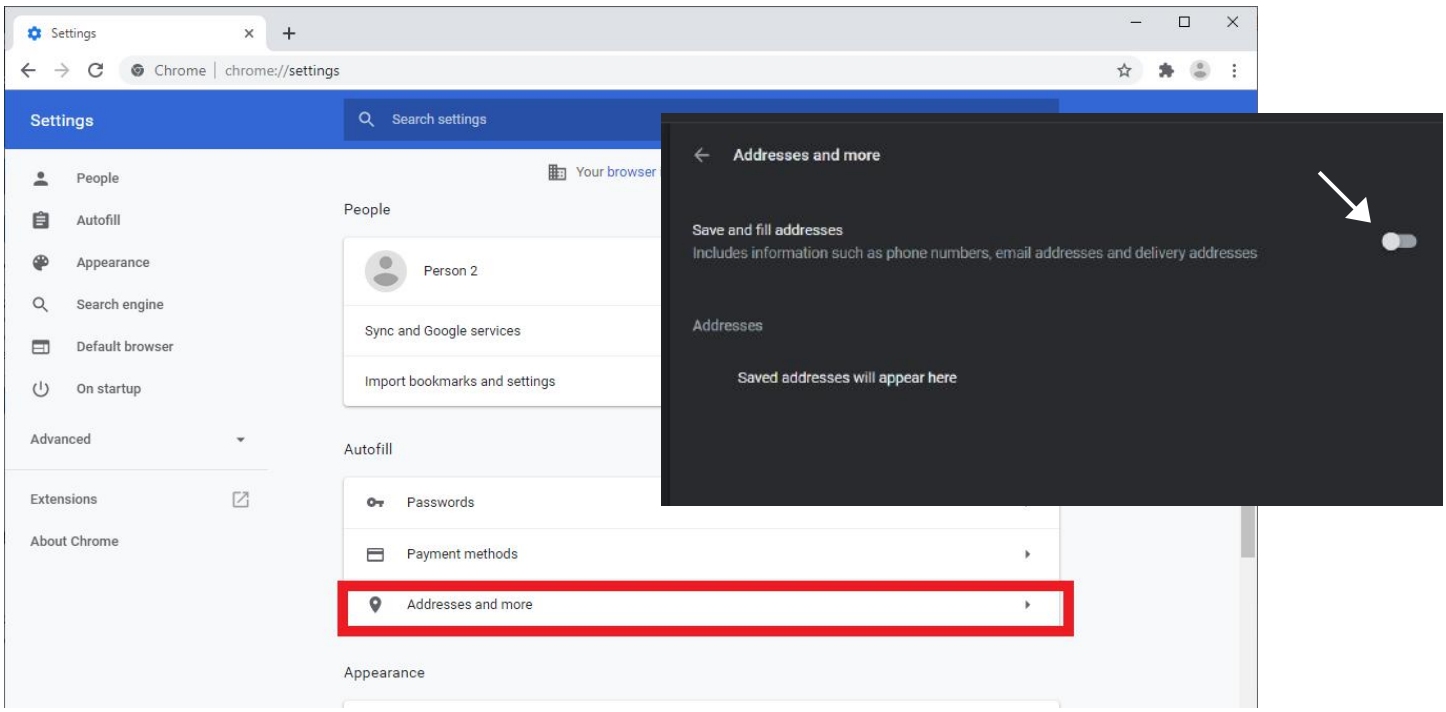
It is recommended that you do not store payment methods in your web browser



Stored Addresses

These browsers can store your addresses in an easily readable format - these can be found by anyone who has access to your browser

To find the addresses your browser currently has saved, go to the 'Addresses and more' section of your 'Settings' menu - here you can turn off the option for the browser to save addresses



Digital Footprint

WHAT IS A DIGITAL FOOTPRINT?

A trail of information that you leave behind when using the internet

People are then able to find information about you by inspecting that trail

The risk of having trails is that it may reveal too much about you, both positively and negatively

Employers want to know more about who they hired, so recruiters will often do an online search of the potential employees

Stalkers will look for any information that they can obtain about their victim, both the victim's online information, and anyone connected to the victim, e.g. family and friends

WHAT CAN YOU DO?

- Search yourself online
- Deactivate and delete
- Check your privacy settings
- Review your profiles
- Think before you post

This way you are able to see what can be found out about you online

Make sure you know what information you are sharing by checking the privacy settings of your accounts

If you no longer use a certain app or account then delete both - this means it can't be found and prevents it from being hacked without you knowing

Take some time to go through the things you have posted and delete anything that can have a negative impact on you

Before you post something about yourself or others, think about how much information you're sharing and who can see it

MANAGING THE RISKS

Report content

If someone else has posted something about you that gives away too much information, most places allow you to report it

Photo location

Hide all house numbers, street names landmarks or other information that can help locate your whereabouts

Keep personal details private

Don't put identifying information (e.g. your home address) on social media and don't post pictures with personal information in them

Turn off GPS

Don't tag your location on pictures and turn off geotagging so that information about your location isn't added to your photo files

Information leaks

Even if you tie down your privacy settings, you would need your family and friends to do the same. Have a talk with them about sharing pictures or posts about you

Moving address

Remember to update your address for all the mail you have signed up for so that your mail doesn't get sent to the wrong house

Understanding

Social networks provide support and comfort, which makes it hard to leave social media behind, just keep in mind your online safety

Mobile Malware

WHAT IS MALWARE?

Software that is designed to disrupt, damage or gain unauthorised access to a computer system

HOW DO YOU PROTECT YOURSELF?

Installing and scanning with an anti-virus on your device, this will help you identify and remove any malicious software

These symptoms could also be due to the age of your device, it is still recommended to install and activate anti-virus software

HOW DO YOU KNOW IF THERE IS MALWARE ON YOUR DEVICE?

Watch out for these signs:

- Your battery drains much quicker than normal
- Unexplained apps appear on your device
- Increased data usage without your knowledge
- Your device begins to overheat
- Your device becomes slower than normal
- Adverts appear in the notification bar
- Your contacts or you receive strange messages or emails
- Unknown charges to your account

Screenshots

Sometimes we might need to provide evidence of online harassment, which usually consists of social media messages etc, however many messages can now be deleted by the offender, and some platforms automatically delete messages. To help record this evidence you can take a screenshot, of your device, which is a photo of the screen, and you can provide these captures to others, which helps prove the offending behaviour.

CAPTURE 1

Screenshot anything that can be deleted

Important Information can include:

- Usernames
- Messages
- Social Media Posts
- Dates & Times

STORAGE 2

Make sure to safely and securely store your screenshots

It is recommended to keep a backup (copy) of your screenshots on a separate physical location such as the cloud

ACCESS 3

Make sure that access to your screenshots is restricted

- Use strong passwords
- Use strong encryption
- Do not grant access to those who don't need it

Backups

A backup is when you make copies of important information so that they can be recovered/restored if there is loss or damage to the original

Identify the important information you would like to backup e.g. screenshots, identifiable documents, family photos etc.

Identify your devices backup provider and register or login to gain access to your backup space

Start backing up the important information and make sure to test that the backup works by trying to re-download something

Ensure to periodically backup your information especially if there are any changes to the important information you have already backed up

It is recommended to keep backups on a separate physical location to the original data such as on the cloud

How to back up on Apple Devices

How to backup on Android Devices

Set strong passwords for your backups

Make sure to enable two factor authentication if available for an extra layer of security

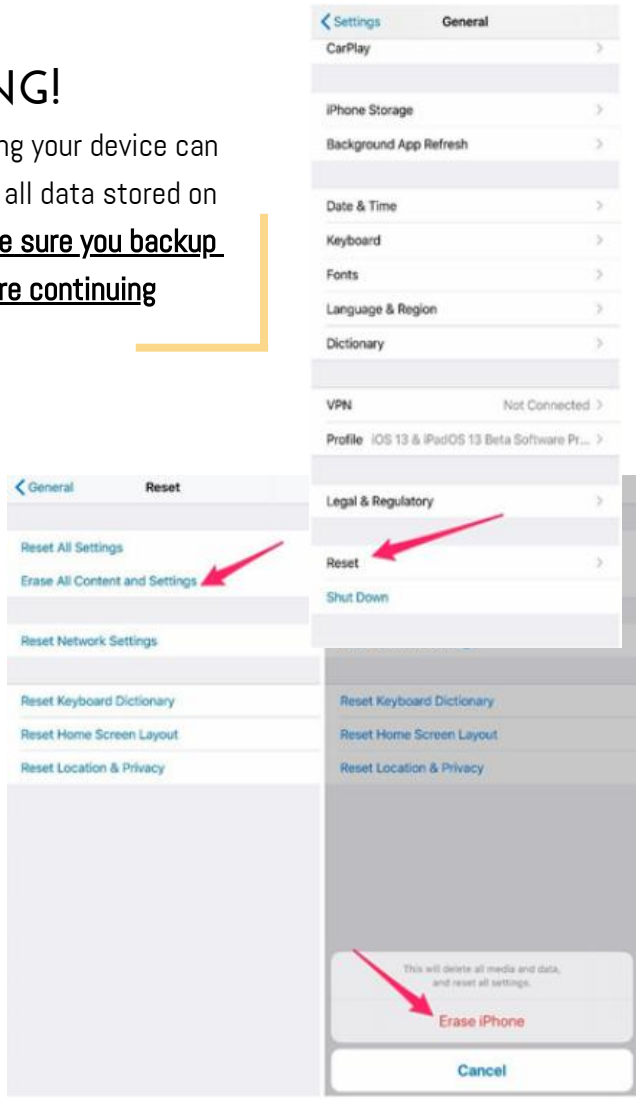
Make sure to restrict access to only yourself or those who need access to your backups

Factory Reset

A factory reset removes all user data from a device and reverts it back to default settings, it returns the device back to the way it was when it was first purchased - you should do this when selling your device, or prior to disposing of it

WARNING!

Factory reseting your device can lead to loss of all data stored on it. **Please make sure you backup your data before continuing**



IPHONE/IPAD

A factory data reset erases all data from the iPhone/iPad
Note: data stored in your iCloud can be restored

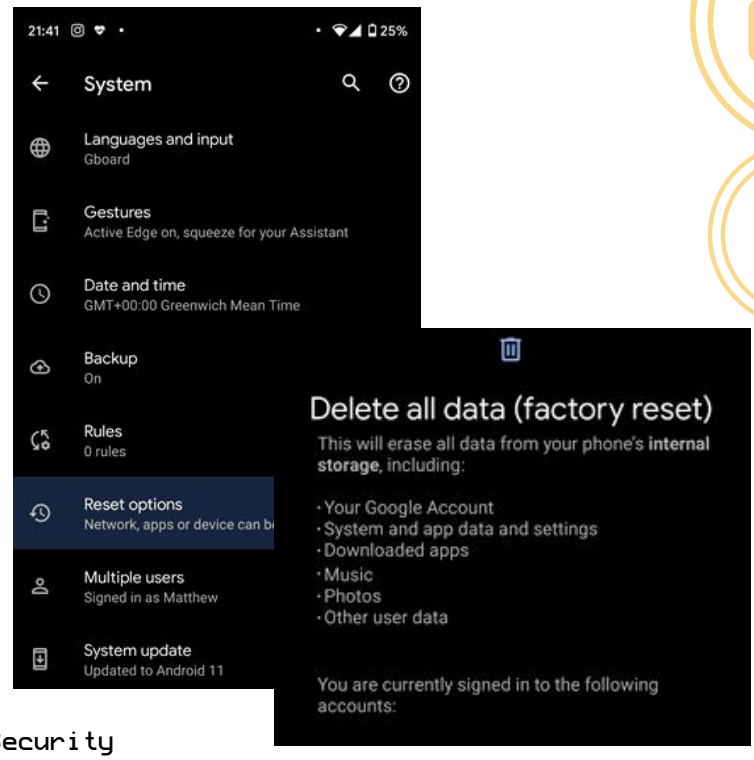
Dependant on settings this can be a lot of the data from the previous install or non at all - check your settings before you start

To reset these devices first access the 'Settings' menu

Next go to the 'General' section, and then select 'Reset' at the bottom of the page

Here choose 'Erase All Content and Settings' and press 'Erase iPhone'

The device will then be wiped of **everything**



ANDROID

A factory reset erases all data from the device
Note: data stored in your Google Account can be restored

To reset these devices first access the 'Settings' menu

Next go to the 'System' section, and then select 'Reset options'

Here choose 'Delete all data (factory reset)', you may have to type in you password

The device will then be wiped of **everything** - you can then sign into your account to restore your data from a backup

SAMSUNG

A factory reset erases all data from the device
Note: data stored in your Google Account can be restored

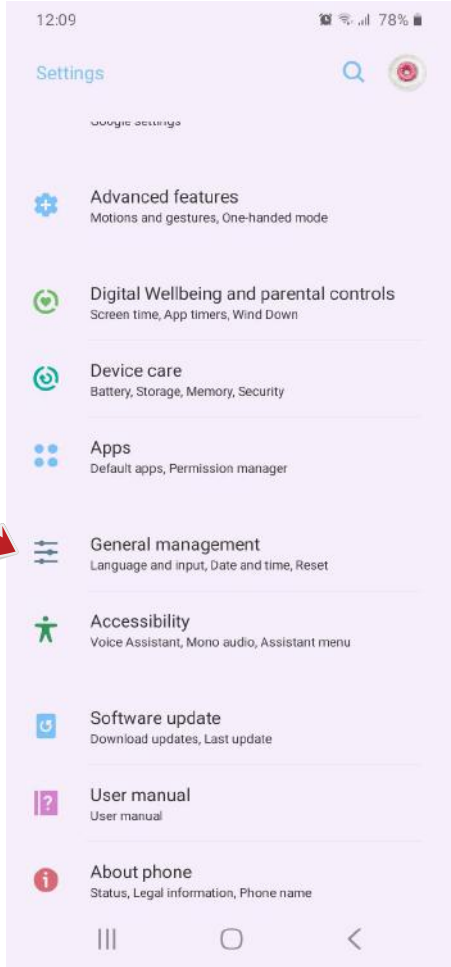
To reset these devices first access the 'Settings' menu

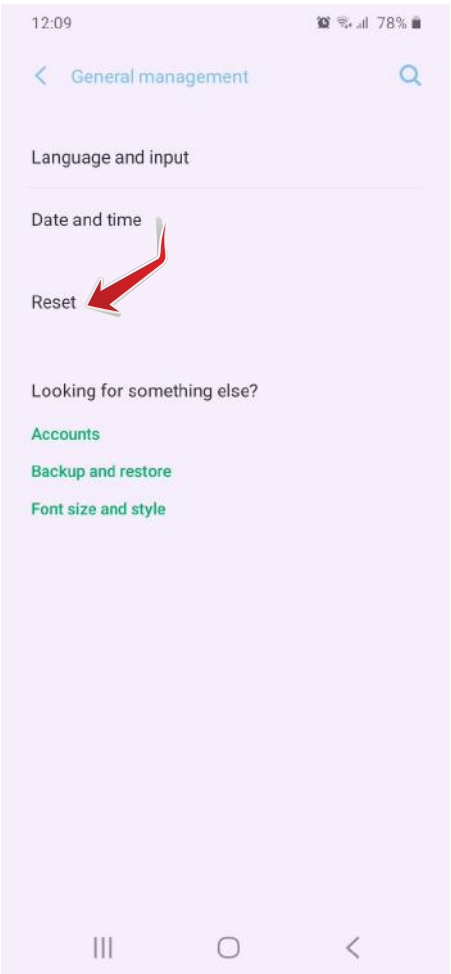
Next go to the 'General Management' section, and then select 'Reset'

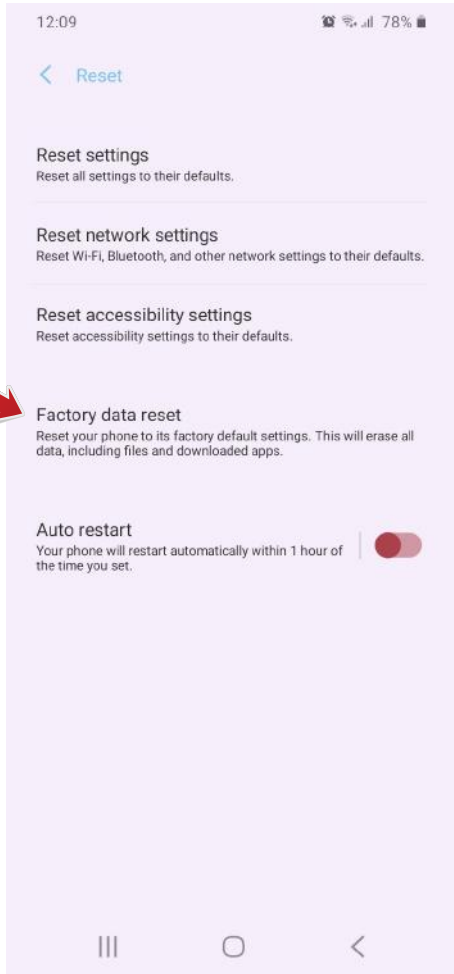
Here choose 'Factory data reset'

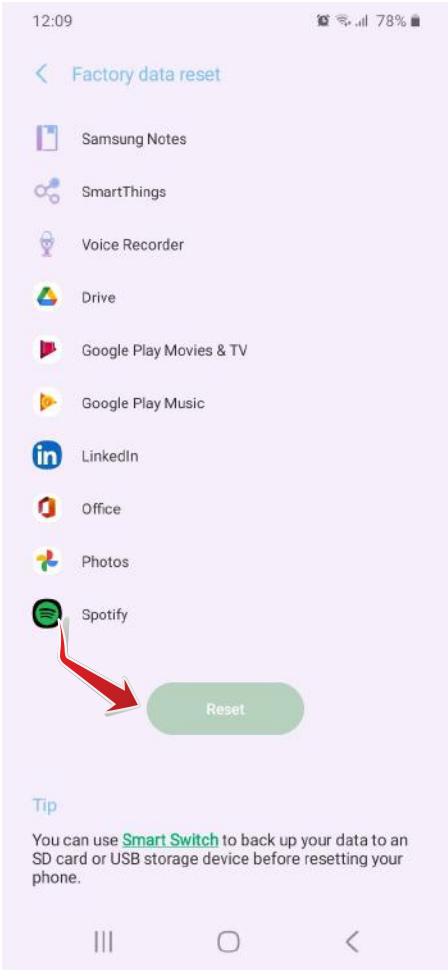
In the next section scroll to the bottom and press the 'Reset' button

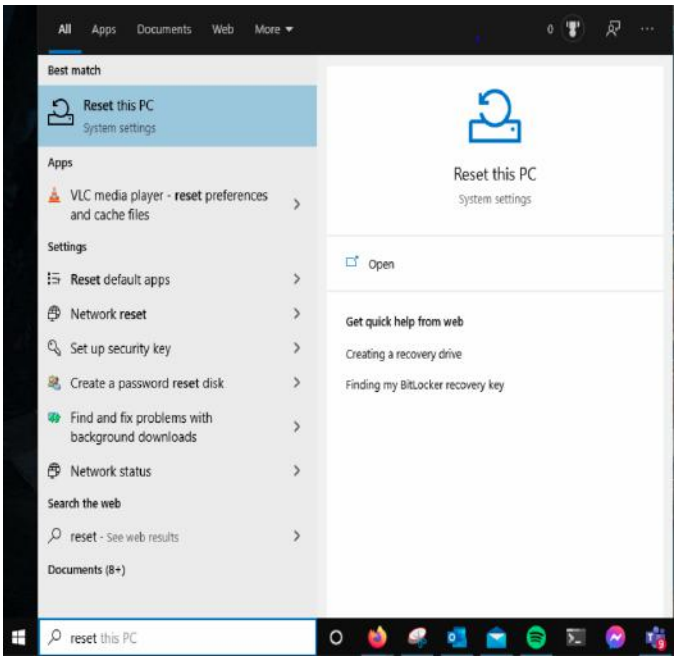
The device will then be wiped of **everything**

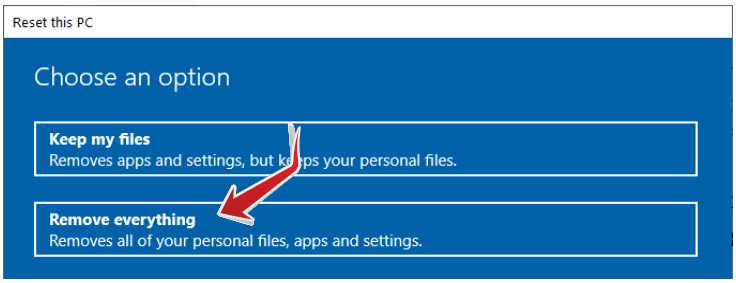












WINDOWS PC

A factory reset erases all data from the device

Devices that run Windows have a reset tool

Access this through 'Settings' and then the 'Recovery' section

Here you should see the heading 'Reset this PC', select the button under this labelled 'Get started'

You will then be asked whether you would like to keep the files on your device or remove them, choose 'Remove everything'

The device will then be wiped of **everything** - this includes accounts for programs and any passwords saved in your browser

MACBOOK/MAC DESKTOP

A factory reset erases all data from the device. Note: the Macbook and Mac reset processes have more steps than previous

Select the apple symbol in the top left corner of your screen and select 'Restart'

Whilst the computer is restarting, hold down the 'Command' and 'R' keys on your keyboard

A menu labelled 'Recovery mode' will appear, here press 'Disk Utility'

Highlight the 'Macintosh HD' disk, then select 'Erase'

A pop-up window should appear, within this change the format to 'macOS Extended (Journaled), then press 'Erase' again

Select 'Quit Disk Utility' in the 'Disk Utilities' menu

A window will appear giving the option to reinstall macOS, choose 'Install macOS'

Once this new macOS is installed, your computer has been successfully reset to factory settings

Online Child Safety

Set parental controls on your broadband and mobile networks to ensure your child is only accessing age appropriate content

Note: Children must be 13+ to access major social media websites

Encourage your child to use their tech devices in the same spaces as you to keep an eye on them

Make sure your child knows **not to share personal information** online, this includes date of birth, location, full name, and mobile number

Note: You can disable location services so your child doesn't unintentionally share their location

Ensure your child is only talking to **real-life trustworthy family and friends** online

Make sure that your child is only logging onto websites **through a children's account that is managed by you**

Note: Make sure children cannot access your accounts, and they do not know your passwords

Use two-factor authentication which means if your child gets your password they still can't access the account or service

Download age appropriate apps you are happy for your child to use

A group of settings that, when combined with privacy settings,

Pare
Cont

What ar
trying to

Advice by Age?

Remember - social media's have age requirements for a reason

Online Gaming Advice Hub

Whilst some caution is needed to maintain safety and healthy gaming habits, remember that online gaming can have a positive impact on children's development and socialisation skills - you don't have to have the top tech for this. Communication and involvement are important for both parents/carers and children.

Lots of games have age ratings to help you out

Social Media Guide

You can encourage and support your teen in navigating the benefits and risks of social media. Helping them understand problems such as cyberbullying and location sharing whilst allowing them freedom to develop creativity, wellbeing, and keep in touch with family and friends.

General Guides and Resources?

These skills will constantly be evolving and changing as technology does

Digital Resilience Toolkit

In a world where technology is increasingly important, learning digital resilience is a skill you can help your children grow. Their needs will change as they get older but it is important to continue helping them learn to stay safe.

They can even make everyday tasks fun and accessible

Guide to Apps

Similar to online gaming and social media, there are risks to using many apps, however, many can also help you encourage your child to exercise, learn and look after their wellbeing. There are also apps that can help you keep your child safe.

Online Money Management Guide

In-game purchases can be risky, with children not understanding what they are doing and accidentally generating large bills. By understanding in-game currencies and spending, you can help teach your children about the value of money, how to make informed purchasing decisions, and how to have good money management skills.

Lots of games are free to download, but include in-game purchases

Guide to Buying Tech

Understanding what your child needs when it comes to technology can be difficult, especially if you're not very tech savvy. It's important to consider what is age appropriate and how their e-safety can be maintained. Help them understand how to use the tech, and how to keep themselves and it safe and secure.

You don't need to have the latest or most expensive tech for it to be entertaining and safe

Set Up Safe Device Checklist

There are important factors to consider when setting up a device for your child, including: proper setup (with the required parental controls), disabling or password protecting necessary features, and discussing security measures with your child to ensure they understand how to keep themselves safe.

Remember to setup necessary controls on your broadband and mobile networks too

put you in control of what your child can see or experience on the internet

ntal
trols

re you
o find?

Information about online issues?

Smartphones and devices

- Controls can be found in the device settings
- Can be used to restrict specific aspects - from screen time to downloading apps
- Additional apps & software can be downloaded
- **Does not** restrict content on apps or the internet

Social Media

- The majority of controls can be found in Settings
- Person specific restrictions (e.g. blocking, reporting) are usually on **their** profile
- Access to the platform often requires an account and use of an app or device
- Restrictions can apply to privacy, content, external applications etc
- Some sites involve live features, including video content, this increases the risk of children viewing inappropriate materials, caution is advised

Tech savvy children can get around some of this - see our Online Child Safety guide

Setting Controls?

Broadband and Mobile Networks

- Restrictions often require manual setup
- Mobile network restrictions do not restrict on Wi-Fi
- Controls range from tailored content restrictions to purchasing and location settings to file sharing, gaming, contact and malware
- Often found through package settings, account details or a phone call/text
- Requirements: account and relevant details, phone number

Some providers automatically set

Occasionally require secondary software

Entertainment and Search Engines

- Controls are often found in a Settings menu
- Controls are occasionally found with setup details, relevant buttons or related web pages
- Most work across all areas of the service, some are device or show/chat specific
- Most only need internet access and account details
- Restrictions range from setting pins, restricting inappropriate content, purchasing and time limits to messaging/comments, locations and tailored to children versions of platforms

Can be an icon

Gaming Consoles and Platforms

- Controls are can be found in Settings, an app or under 'Parental Controls'
- Access to the account (or account details, device/console and game are often needed
- Restrictions vary from content and access to time and privacy
- Purchasing controls can also be applied

Some require a 'Parent/Master' account

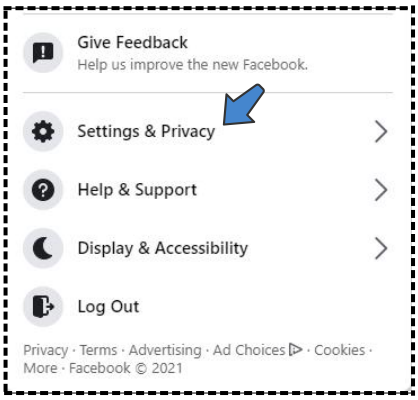
Social Media Privacy Settings

ON

Facebook

1 Settings & Privacy

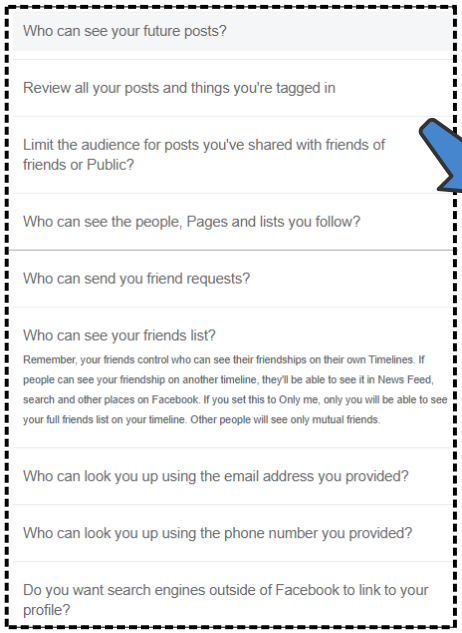
To access your security and privacy settings, click on the small triangle at the top right of the screen, and click on 'Settings & Privacy', then click on 'Settings'

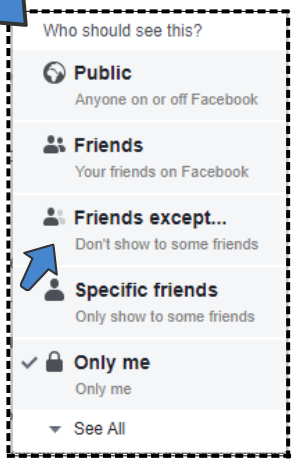


Be careful when sharing your personal information online - it could be used by others to target you

2 Privacy

To change your privacy settings, click on 'Privacy' on the left hand side and adjust them accordingly





3 Security and Login

Set up two-factor authentication by going to the 'Security and Login' menu on the left hand side

Turning this on gives you an extra layer of protection preventing easier access to your accounts

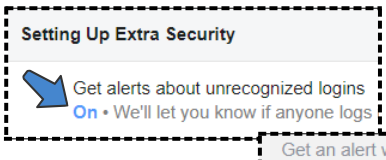
4 When You're Logged In

To check what devices are logged into your account go to 'Security and Login', then 'Where You're Logged In'

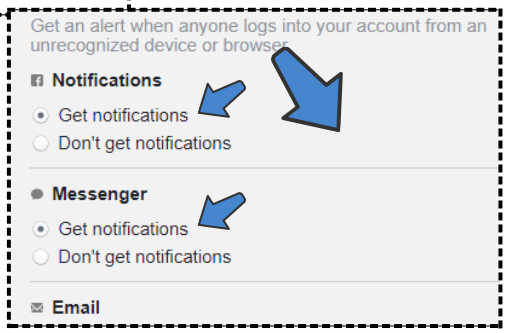
Here you can check what devices are logged into your account, and log out of any if necessary

5 Unrecognised Login Alerts

In 'Security and Login', under 'Setting Up Extra Security' select 'Get alerts about unrecognized logins'



Turn this on to receive a notification if anyone logs in from a device or browser you don't really use

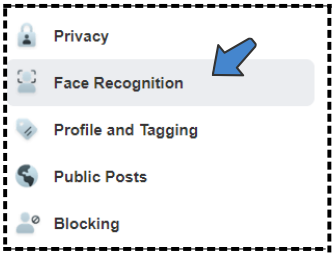


6 Security and Login Shortcut

A quicker way of doing step 3-6, is to click the 'Recommended' section in Security and Login, this option will take you through these steps

7 Turn Off Facial Recognition

To stop Facebook from creating a template of your face and comparing it to other images, to see if you might appear elsewhere, turn off the 'Face Recognition' setting



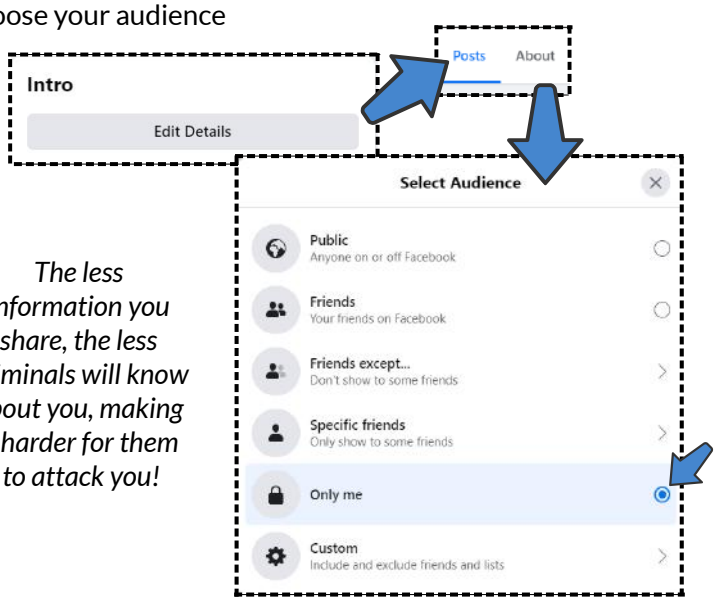
Leaving this on makes it easier to have your biometrics stolen

8 Stop Being Tagged

Under 'Profile and Tagging' edit these settings to prevent unwanted tags, a good choice is to enable reviewing before it gets posted. This allows you to decide whether something about you is posted or not

9 Personal Information

- Go to your profile by clicking your name and click edit details on the left side of the screen
- You can click "about" as well to check and change what details you have shared
- Click on the small privacy icon next to each option to choose your audience



The less information you share, the less criminals will know about you, making it harder for them to attack you!

10 Location

Select 'Location' on the left and turn this Off.
This setting allows Facebook to compile a log of the precise location you've been to while using your device

Leaving this on makes it possible for stalkers or those who have access to your account to precisely track your location, where you go and when

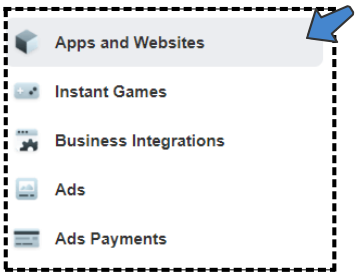
11 Remove Your Profile From Google Results

The very last option under 'Privacy' has a setting where you can disable search engines outside of Facebook from linking to your profile

12 Apps and Websites

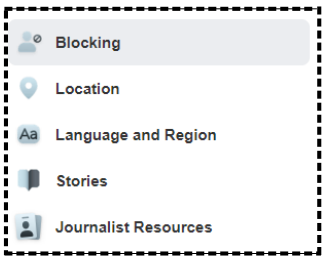
Get rid of any games you are no longer using in 'Apps and Websites' by checking the white tick box and then clicking remove

These Apps and Websites linked to your Facebook account that you no longer use, still have access to your Facebook data. If these become bugged or hacked, you may face security leaks



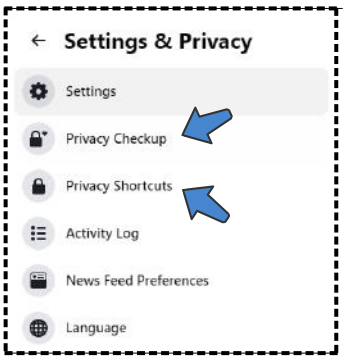
13 Blocking

Blocking disables any and all communication between the two of you on Facebook, they wouldn't even be able to search for you, you'd be invisible to them



14 Alternative Methods

When clicking the little triangle in the top right, click 'Settings & Privacy' and have a look at 'Privacy Checkup' and 'Privacy Shortcuts'



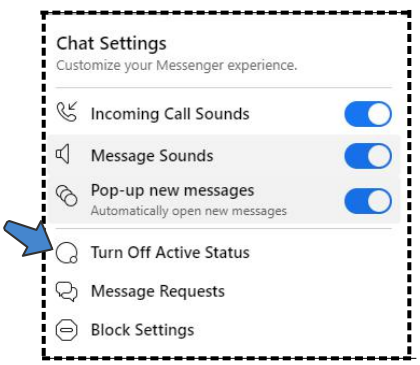
15 Public Posts

Under 'Public Posts' there's an option about who can follow you, turn this to friends

There are more options on this page regarding who can do what to your public profile

This is important to consider because you don't want people you don't know commenting on your profile

16 Active Status



To avoid people knowing when you're online, go to the top right of your screen and click the chat bubble, followed by the 3 dots, here you can 'Turn Off Active Status' (when you're on facebook)

Social Media Privacy Settings

ON

Whatsapp

Be careful when sharing your personal information online - it could be used by others to target you

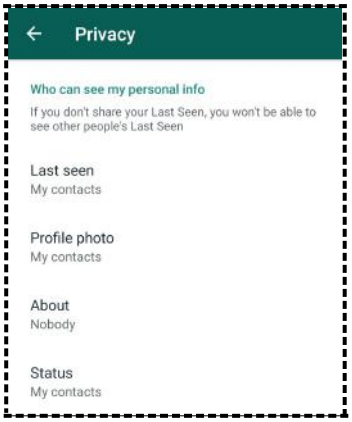
1 Settings & Privacy

To access Settings, click on the 3 dots on the top right and click on 'Settings'

2 Privacy

Click on 'Account' and then 'Privacy', here you can decide who sees what about you:

- Your last seen status
- Your profile photo
- Your about
- Your status

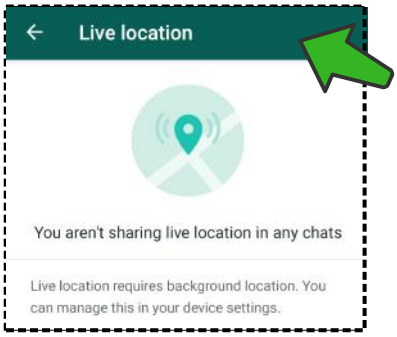


3 Groups

In 'Privacy' there is another option regarding who can add you to groups. Those who you don't allow, will be able to invite you privately, so you can choose whether to join or not

You'll need to press 'Done' when you've adjusted the settings

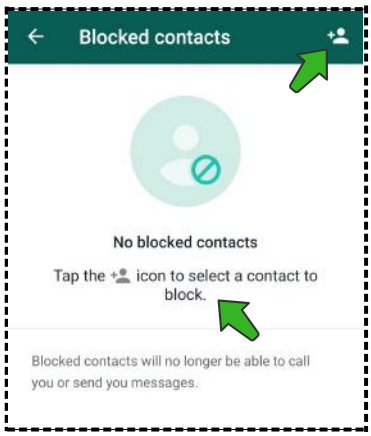
4 Live Location



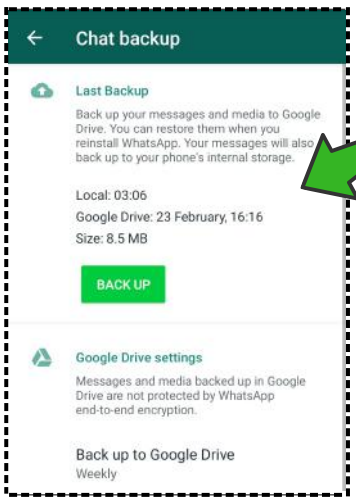
To stop people from seeing your real time location, go to 'Privacy' and then 'Live Location', set this as 'None'

5 Blocking

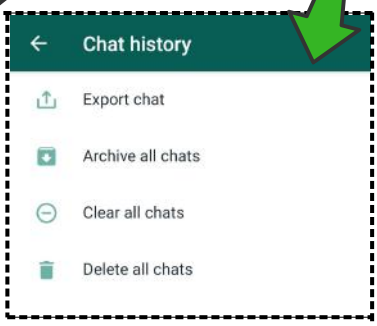
To stop receiving messages, calls, and status updates from a contact, go to the 'Privacy' menu followed by 'Blocked Contacts' and follow the on-screen instructions to block them



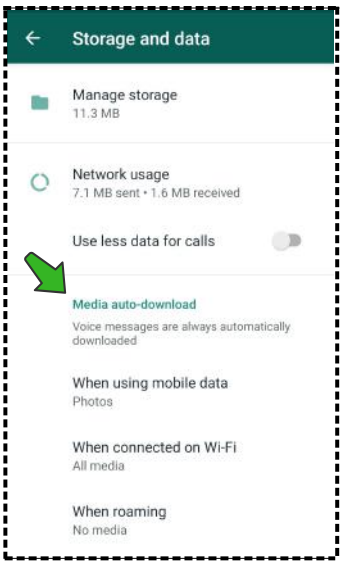
6 Clear History and Backups



In 'Settings' and 'Chats' scroll down and there are two options, 'Chat backup' and 'Chat history'. You can click them and have a look at the options

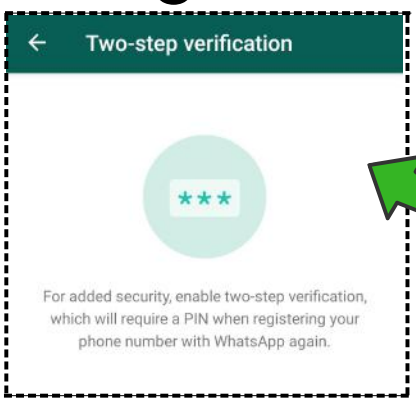


7 Auto-Download



In 'Settings' and 'Storage and data' under the heading 'Media auto-download' you can decide whether to automatically save any incoming photos/ videos

8 Two-Step Verification



In 'Settings' and 'Account' there is an option called 'Two-step verification'

Turning this on gives you an extra layer of security

Social Media Privacy Settings

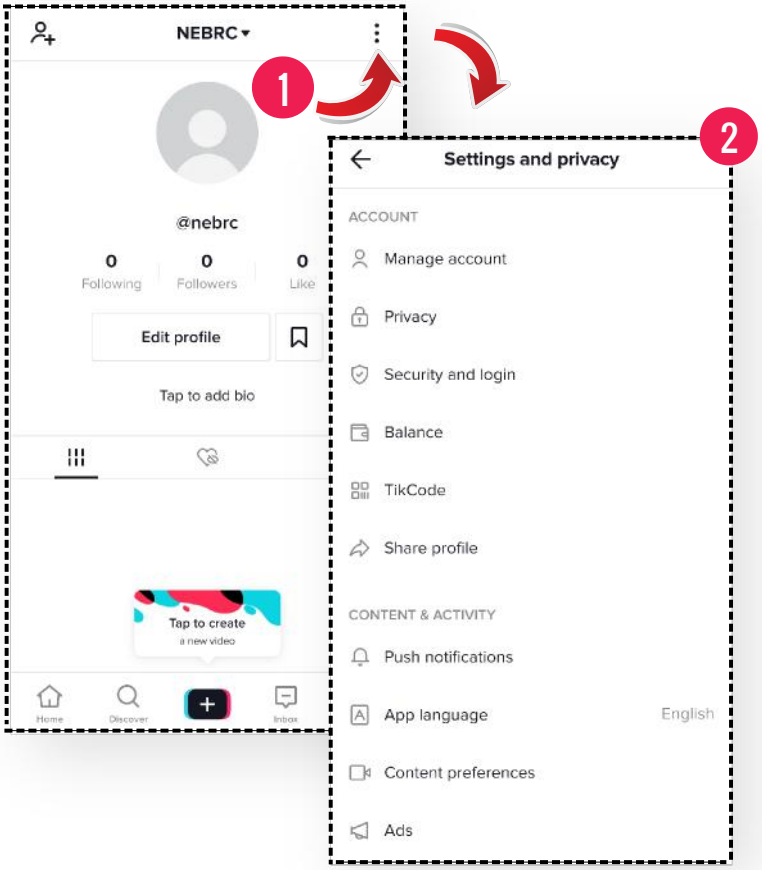
ON

TikTok

Be careful when sharing your personal information online - it could be used by others to target you

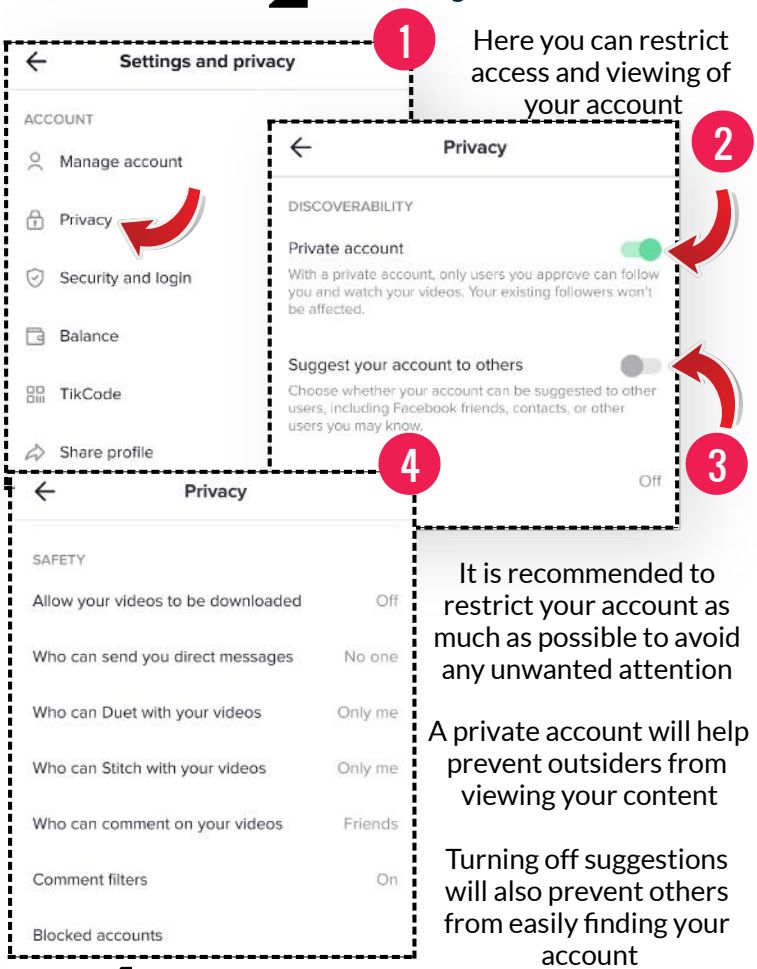
1 Settings & Privacy

Go to your profile page and click on the 3 dots to access the "Settings and privacy" menu



2 Privacy

Here you can restrict access and viewing of your account

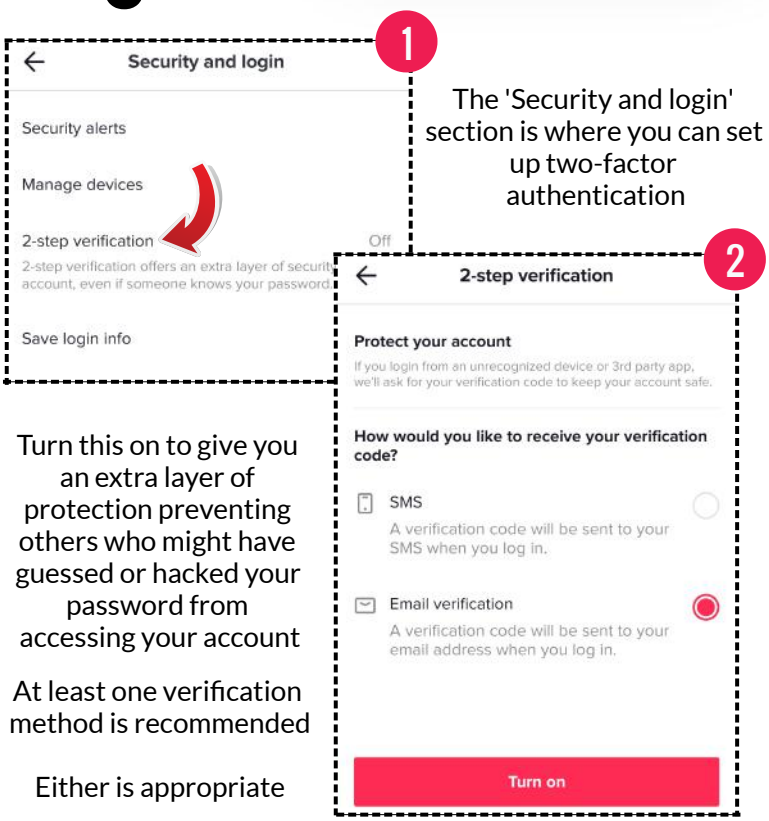


It is recommended to restrict your account as much as possible to avoid any unwanted attention

A private account will help prevent outsiders from viewing your content

Turning off suggestions will also prevent others from easily finding your account

3 Two-Factor Authentication



The 'Security and login' section is where you can set up two-factor authentication

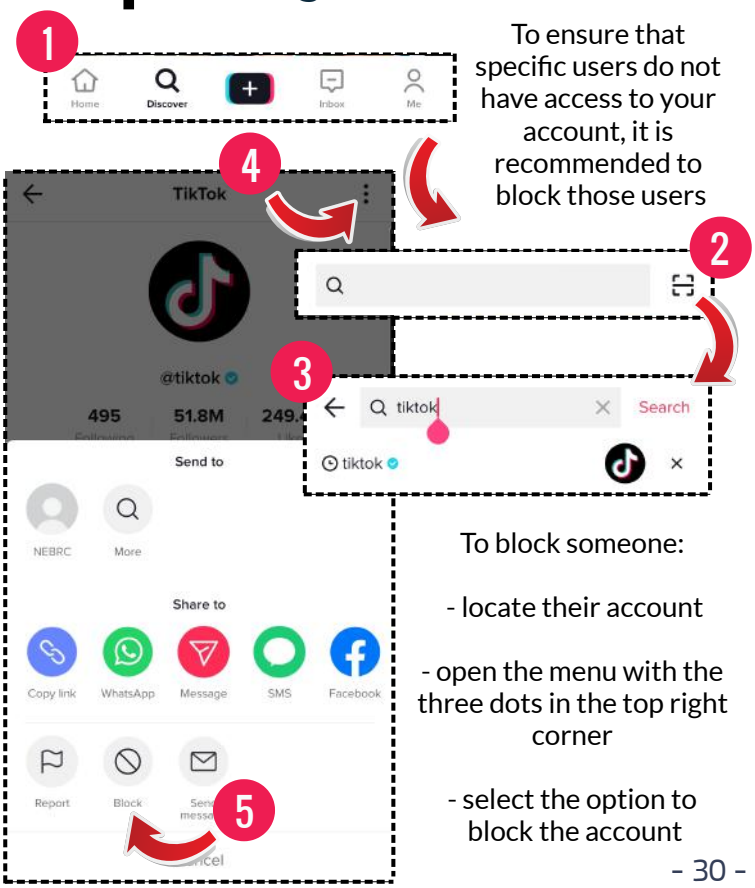
Turn this on to give you an extra layer of protection preventing others who might have guessed or hacked your password from accessing your account

At least one verification method is recommended

Either is appropriate

4 Blocking Accounts

To ensure that specific users do not have access to your account, it is recommended to block those users



To block someone:

- locate their account

- open the menu with the three dots in the top right corner

- select the option to block the account

Social Media Privacy Settings

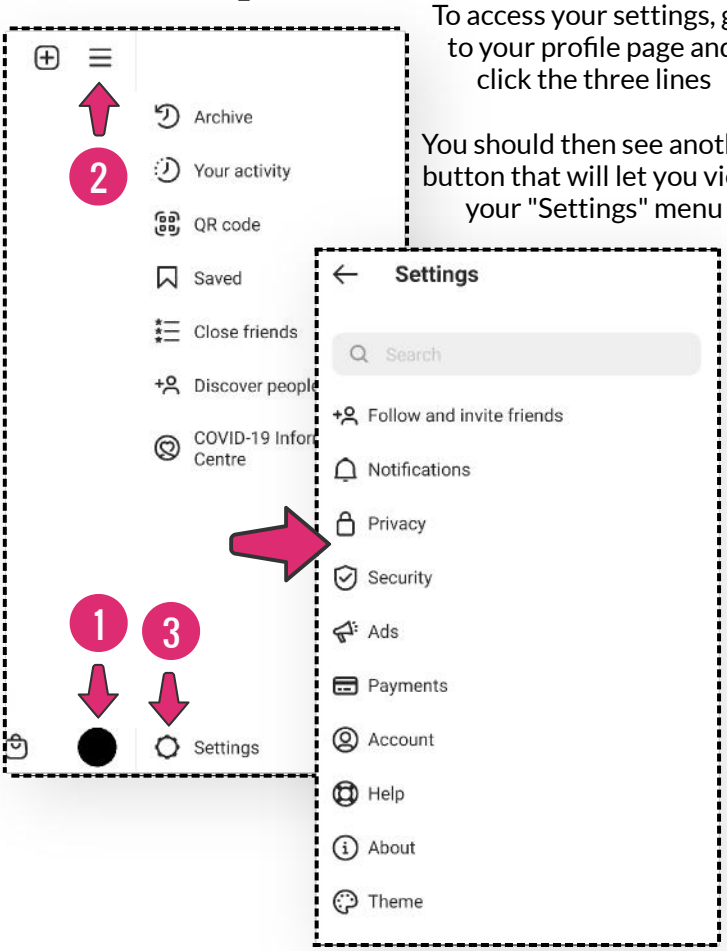
ON *Instagram*

Be careful when sharing your personal information online - it could be used by others to target you

1 Settings

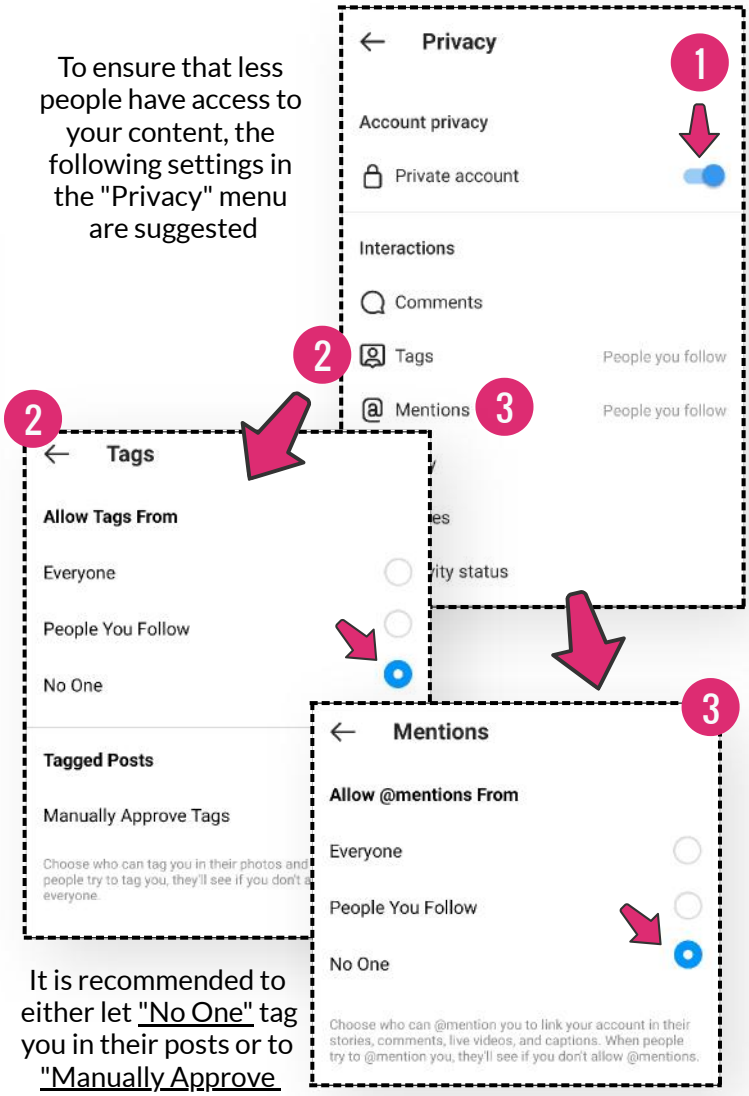
To access your settings, go to your profile page and click the three lines

You should then see another button that will let you view your "Settings" menu



2 Privacy

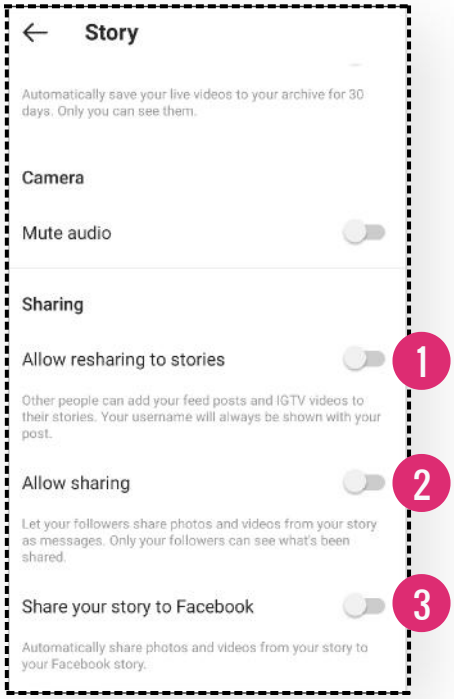
To ensure that less people have access to your content, the following settings in the "Privacy" menu are suggested



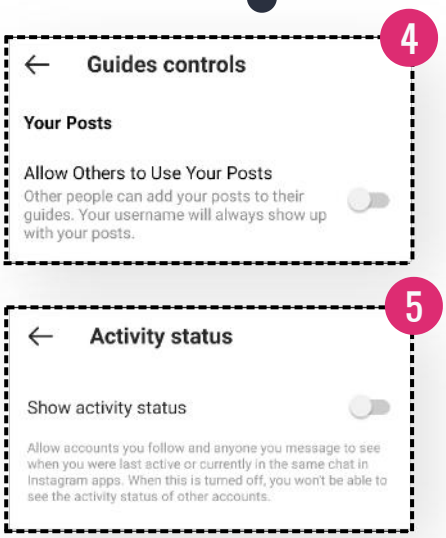
It is recommended to either let "No One" tag you in their posts or to "Manually Approve Tags" so that you have more control of your image on other people's profiles

It is also recommended to restrict mentions to "No One" so that people do not have quick access to your account through other people's accounts

3 Stories, Guides and Activity Status



In the 'Privacy' menu, ensure that the 'Story' and 'Guides' sub-menus restrict story sharing settings to prevent views from unwanted accounts



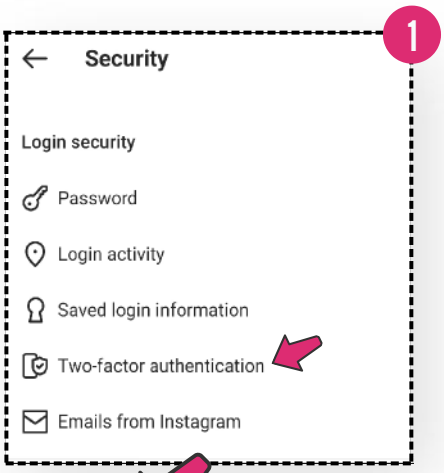
Do not location tag your content

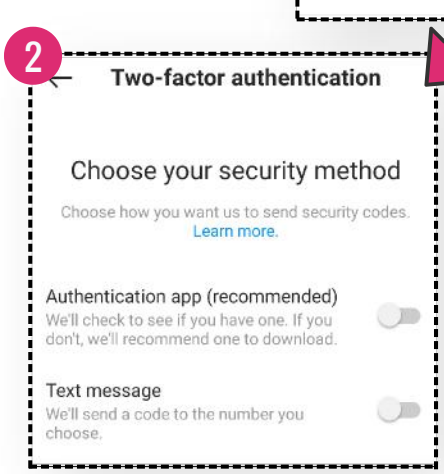
Do not post content that can compromise your location

Do not follow suspicious accounts

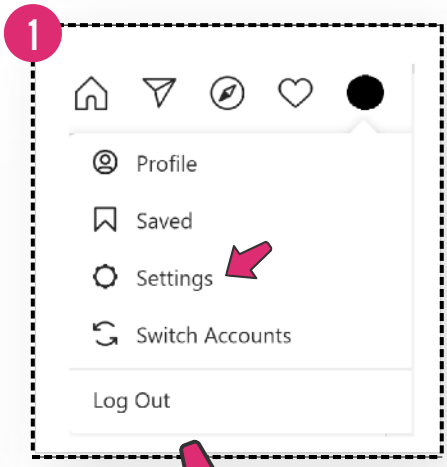
4 Two-Factor Authentication

Enable Two-factor authentication as an extra layer of security, this prevents others who might have guessed or hacked your password from accessing your account

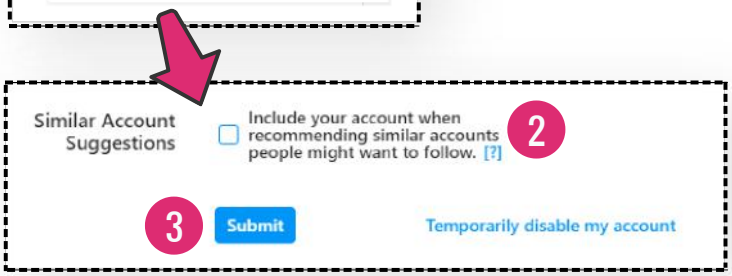




5 Restricting Account Suggestions



To prevent your account being recommended to other people, turn off the 'Similar Account Suggestions' setting

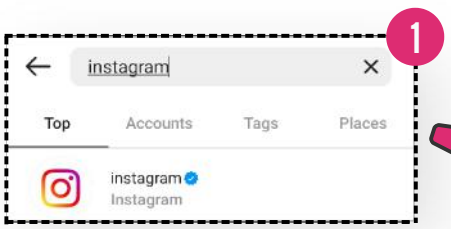


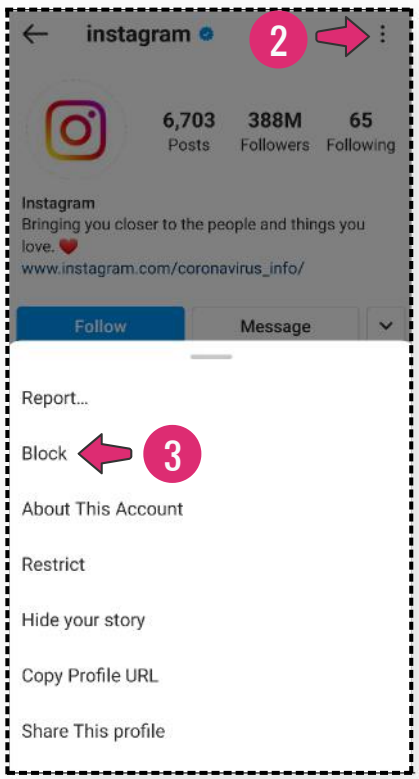
You must be logged into Instagram through its website page to change this setting.
You cannot access this setting via the mobile application

6 Blocking

It is advised to block someone to completely prevent them from viewing your account

First search for and view their account





Blocking V Restricting

- Blocking their account will prevent them from being able to view your account
- Restricting their account prevents others from viewing their interactions on your page but they can still see your account

Therefore, blocking accounts is recommended over restricting them

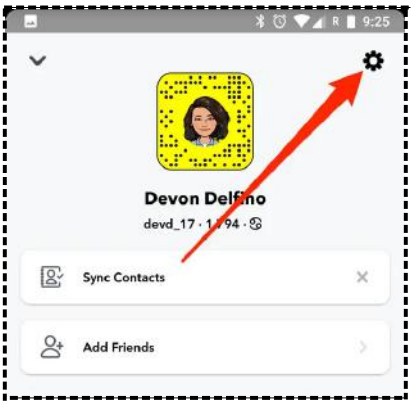
Social Media Privacy Settings

ON

Snapchat

Be careful when sharing your personal information online - it could be used by others to target you

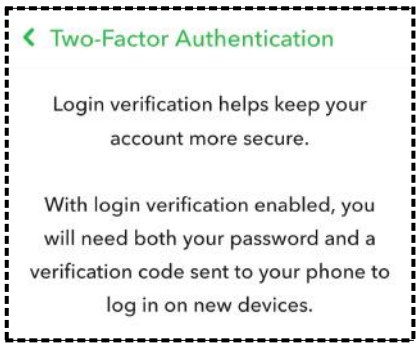
1 Settings



To access 'Settings', click on your icon's picture in the top left of the screen and select the settings icon (the cog)

2 Password and Two-Factor Authentication

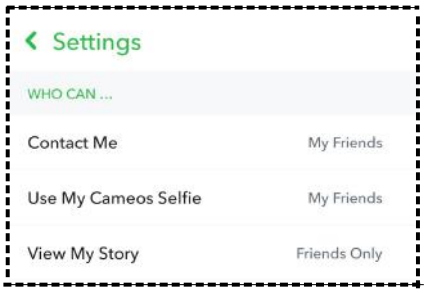
You can change your password and turn on two-factor authentication in Settings



Turn this on for extra security because for someone to get into your account they would need both your password and a verification code that will be sent to your phone when logging in on a new device

3 Who Can

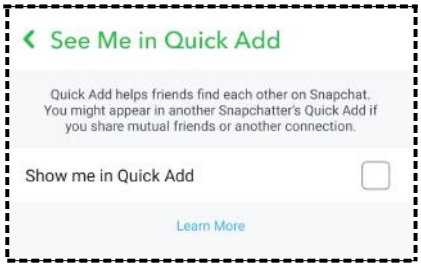
Scroll down to the 'WHO CAN' section, here you can select who can contact you, use your cameos selfie and view your story, it is suggested that you change these to 'Friends Only'



The less information you share, the less criminals will know about you, making it harder for them to attack you!

4 Quick Adds

Under 'WHO CAN' there is the option 'See Me In Quick Add', leave this off as it makes it easier for people to find you if it is on



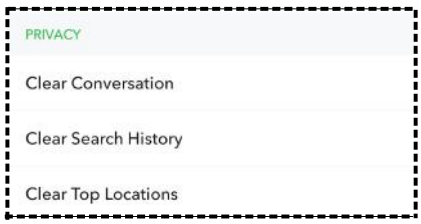
5 Location

It is possible to hide your location by going to 'See My Location' in the 'WHO CAN' section, and turning on 'Ghost Mode'

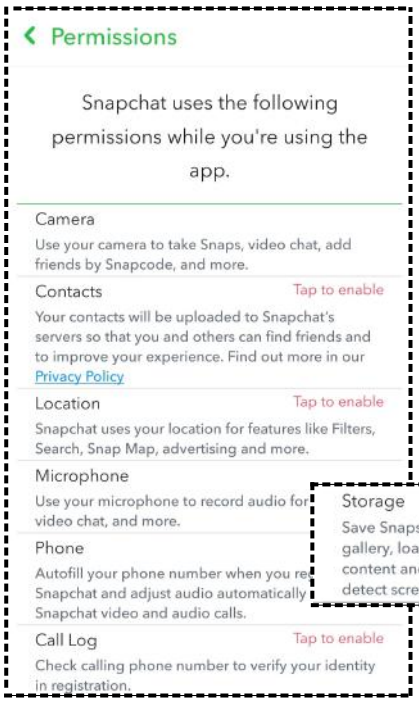
It is suggested to do this in order to keep you safe from potential stalkers

6 Privacy

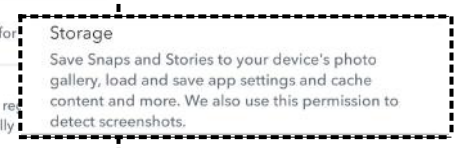
Scroll down to 'PRIVACY' here you can clear your conversations, search history and top locations. This will cover your tracks



7 Permissions

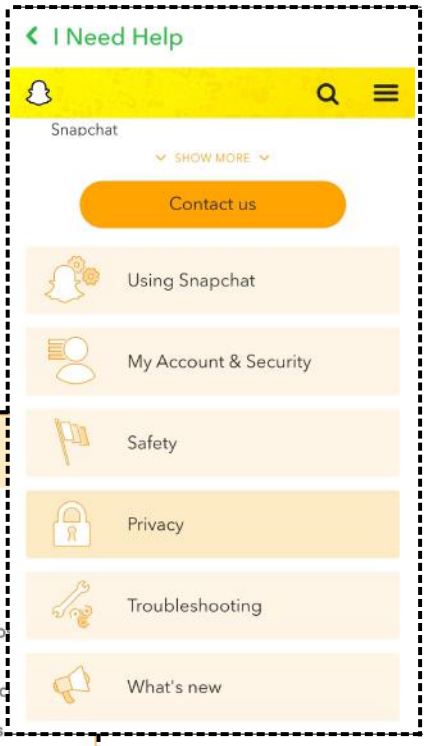


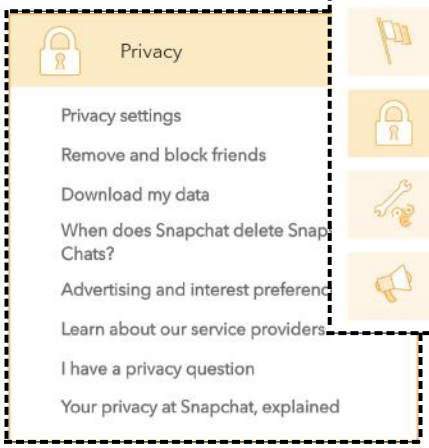
Under 'PRIVACY' go to 'Permissions' here you can see what Snapchat uses while you're using the app



8 Support

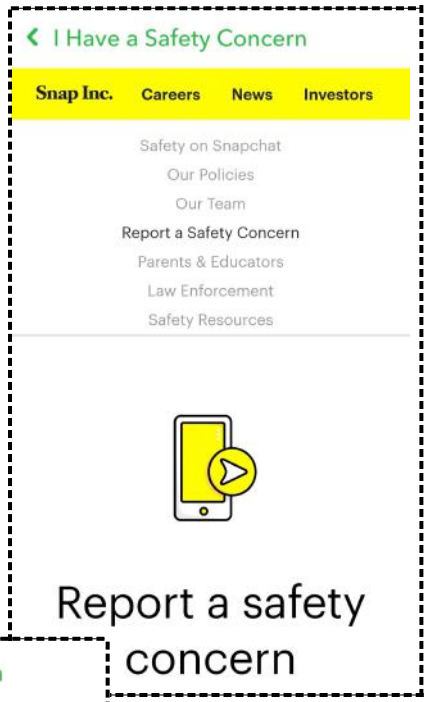
Under 'SUPPORT' you can select 'I Need Help' which gives you more information on all the aspects on Snapchat including 'Privacy'

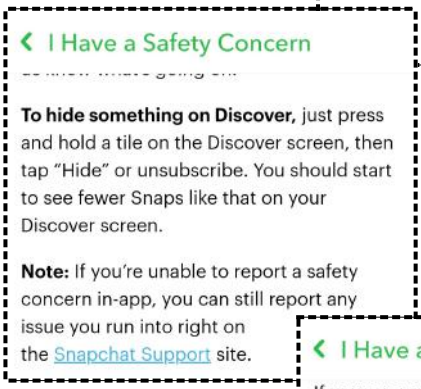




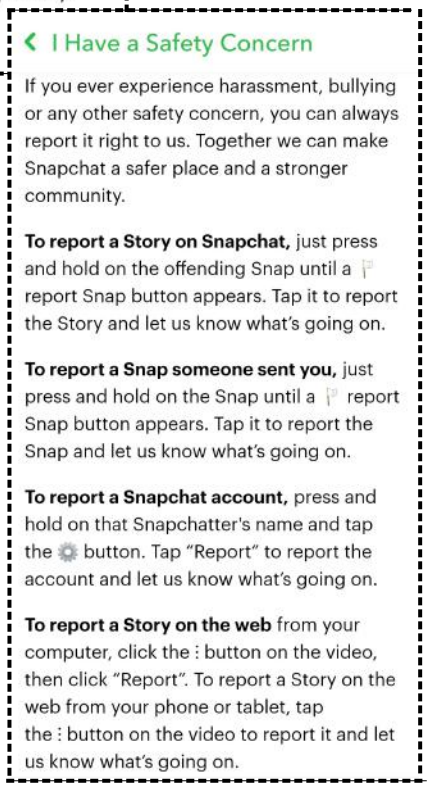
9 Reporting

Under 'SUPPORT' you can select 'I Have a Safety Concern' here it tells you how to report something for the different reasons



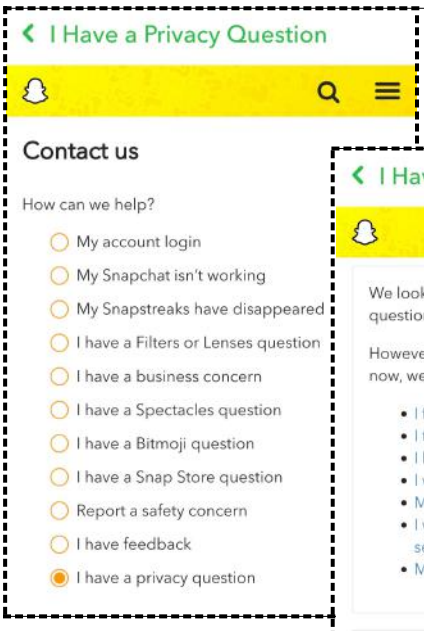


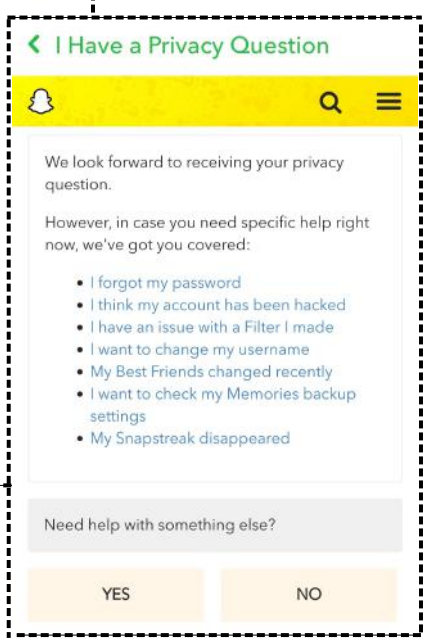
If it's a safety concern, there is a Snapchat Support site



10 Privacy Questions

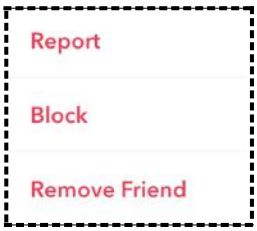
Under 'SUPPORT' you can select 'I Have a Privacy Question' here it helps you with privacy problems you might be facing



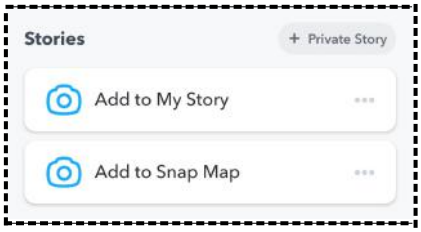


11 Deleting and Blocking

To remove someone or block them, go to the chat screen, tap and hold the contact's name, then tap 'Remove Friend' or 'Block



12 Important!



If you add a post to Snap Map, your location will be seen regardless of Ghost Mode being on, everyone will be able to see this

Social Media Privacy Settings

ON

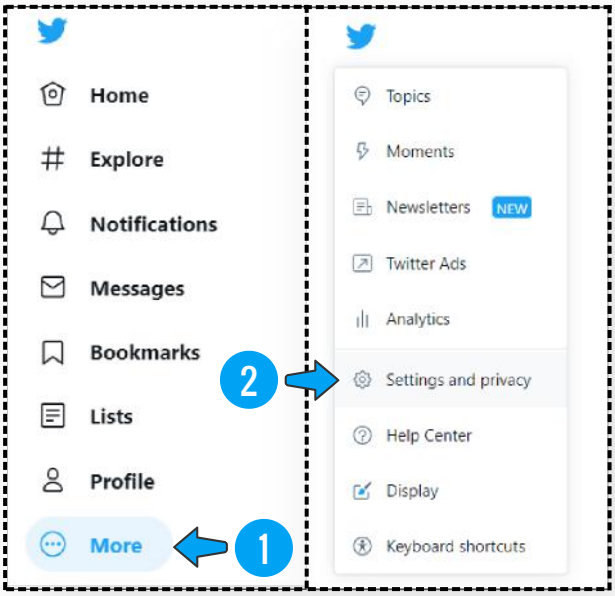
Twitter

Be careful when sharing your personal information online - it could be used by others to target you

1 Settings & Privacy

Click on 'More ' at the bottom of the navigation pane

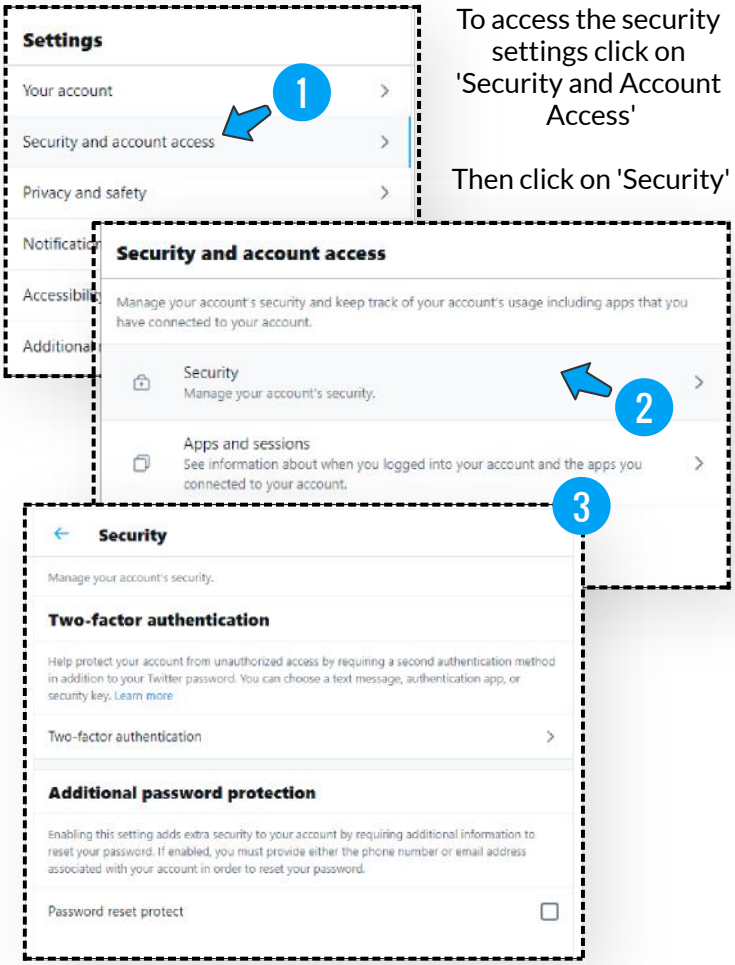
Next click on 'Settings and privacy'



2 Security

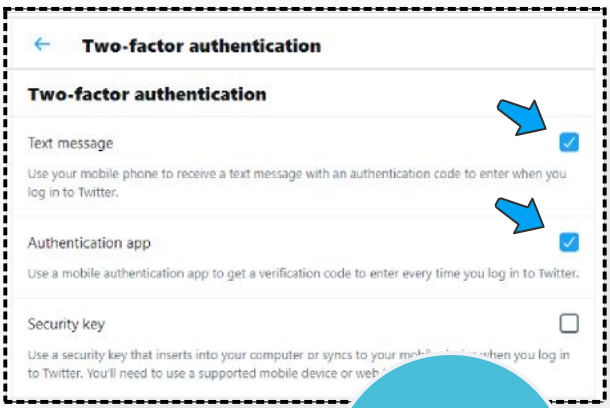
To access the security settings click on 'Security and Account Access'

Then click on 'Security'



3 Two-Factor Authentication

Once in the Security section you can set up 'Two-factor authentication'

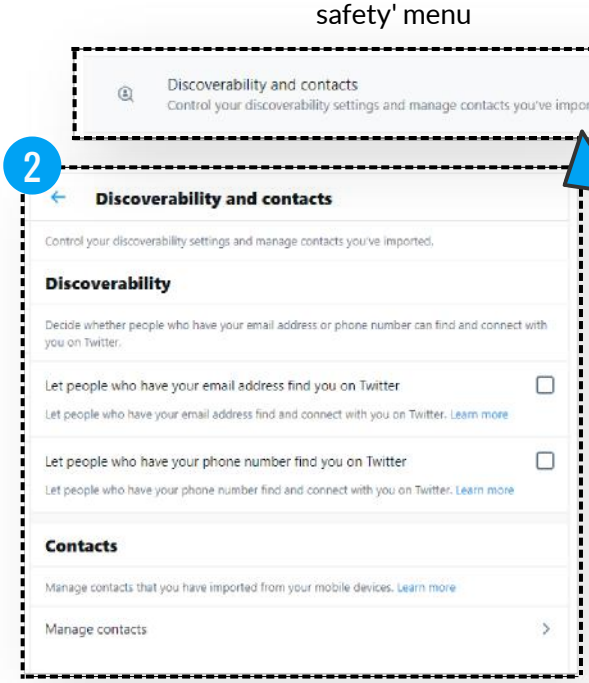


Activating multiple authentication methods is possible. A tick will verify if that method has been activated.

Turning this on can give you an extra layer of protection by requiring approval or an extra identification process - it stops prevents others who might have guessed or hacked your password from accessing your account

4 Discoverability and Contacts

To control who can find you, go to the 'Discoverability and contacts' section which can be found under 'Privacy and safety' menu



Turn these settings off so people who have your details cannot link you back to your account

5 Control Your Direct Messages

To control your Direct Messages (DM's), go to the 'Direct Messages' section from the 'Privacy and safety' menu

1

Direct Messages
Manage who can message you directly.

2

Direct Messages

Manage who can message you directly.

Allow message requests from everyone
Let people who you don't follow send you message requests and add you to group conversations. To reply to their messages, you need to accept the request. Learn more

Filter low-quality messages
Hide message requests that have been detected as being potentially spam or low-quality. These will be sent to a separate inbox at the bottom of your message requests. You can still access them if you want. Learn more

Filter graphic media
Display warnings over messages detected to potentially contain graphic media (like nudity, sexual content, or violence). You'll always have the option to view the media if you want. Learn more

Show read receipts
Let people you're messaging with know when you've seen their messages. Read receipts are not shown on message requests. Learn more

3

Direct Messages

Manage who can message you directly.

Allow message requests from everyone
Let people who you don't follow send you message requests and add you to group conversations. To reply to their messages, you need to accept the request. Learn more

Filter low-quality messages
Hide message requests that have been detected as being potentially spam or low-quality. These will be sent to a separate inbox at the bottom of your message requests. You can still access them if you want. Learn more

Filter graphic media
Display warnings over messages detected to potentially contain graphic media (like nudity, sexual content, or violence). You'll always have the option to view the media if you want. Learn more

Show read receipts
Let people you're messaging with know when you've seen their messages. Read receipts are not shown on message requests. Learn more

Ensure that you don't receive message requests from everyone and that your messages are filtered. Make sure to turn off read receipts to avoid others from seeing you have read their message

6 Blocking Accounts

*To ensure that specific users do not have access to your twitter information, it is recommended to **block** those users*

To block someone, search their account, open 'More' (the three dots) then select 'Block @account'

1

Search Twitter

Recent — Clear all

North East Business Resilience ... @NEBRCentre

2

North East Business Resilience Centre
1,437 Tweets

THE BUSINESS RESILIENCE CENTRE FOR THE NORTH EAST

NEBRC

More — Follow

North East Business Resilience Centre
@NEBRCentre

A non-profit organisation which exists to support and help protect businesses in North East England from cybercrime. Part of the @BRIMCentres network.

3

North East Business Resilience Centre
1,437 Tweets

THE BUSINESS RESILIENCE CENTRE FOR THE NORTH EAST

NEBRC

Following

Turn off Retweets
View Topics
Add/remove @NEBRCentre from Lists
View Lists
View Moments
Share profile via...
Copy link to profile
Mute @NEBRCentre
Block @NEBRCentre
Report @NEBRCentre

Tweets — Likes

4

NEBRC

Blocked

North East Business Resilience Centre
@NEBRCentre
1,985 Following 614 Followers

@NEBRCentre is blocked

Are you sure you want to view these Tweets? Viewing Tweets won't unblock @NEBRCentre. Learn more

View Tweets

To verify if you have successfully blocked someone, go to your settings, then the 'Privacy and Safety' menu and open the 'Mute and block' section

5

Mute and block
Manage the accounts, words, and notifications that you've muted or blocked.

6

Mute and block

Manage the accounts, words, and notifications that you've muted or blocked.

Blocked accounts

7

Blocked accounts

All — Imported

When you block someone, that person won't be able to follow or message you, and you won't see notifications from them. Learn more

North East Business Resilience Centre
@NEBRCentre
Blocked

A non-profit organisation which exists to support and help protect businesses in North East England from cybercrime. Part of the @BRIMCentres network.

Social Media Privacy Settings

ON

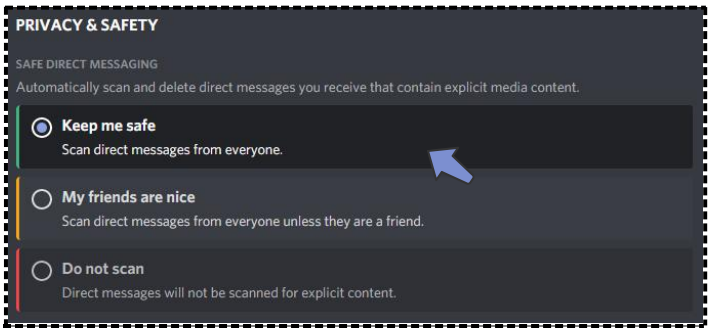
Discord

Be careful when sharing your personal information online - it could be used by others to target you

1 Privacy and Safety

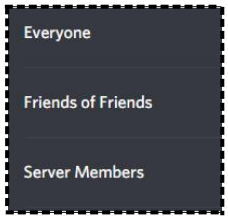
Click on the settings button on the bottom left next to the sound icon, then click on 'Privacy & Safety'

Keep me safe will scan and block explicit content for you



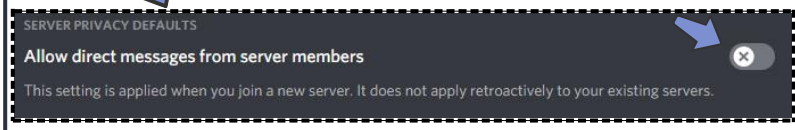
2 Who Can Message or Add You

To change the settings for who can message you, go to 'Privacy and Safety'

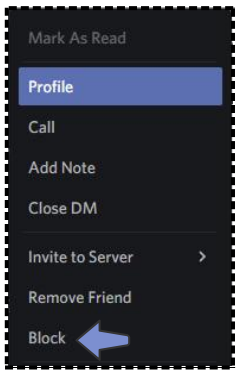


Consider whether to let server members who aren't your friends direct message you

Underneath that you can decide who can add you as a friend, you can even turn it off completely



3 Blocking



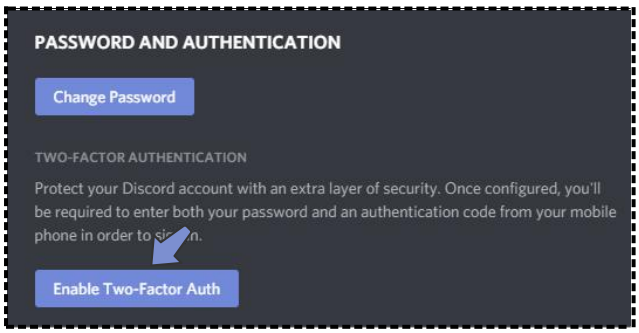
To block a user or chat, right click on them or it, and click 'Block'

This will mean they cannot direct message you

4 Two-Factor Authentication

(2FA)

Enabling two-factor authentication means that your account requires a second process to log you in, this will take the form of a verification code sent directly to your mobile phone that you will be required to input before you can access your account



Go to 'My Account' in the settings menu, and click 'Enable Two-Factor Authentication'

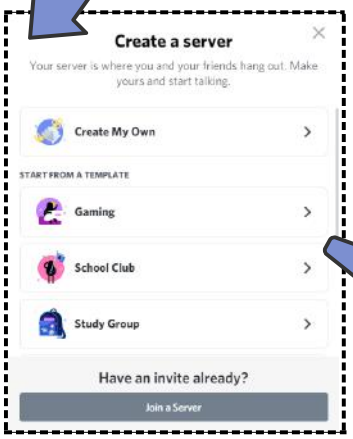
Once this is enabled you can also include SMS Authentication

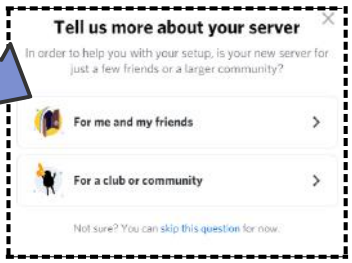
This is very important as it will alert you whenever someone attempts to log into your account, helping prevent it from being hacked

5 Create Your Own Server

To create your own server go to the left hand side of the screen and press the button with a '+' sign

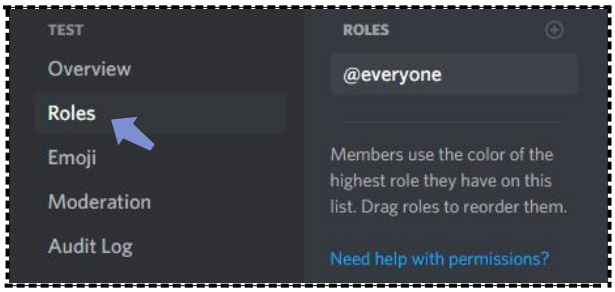
Here you will find steps to customise the server to your preferences





6 Roles and Permissions

To adjust people's roles, go to server settings by clicking on the name of your server and click on 'Roles'



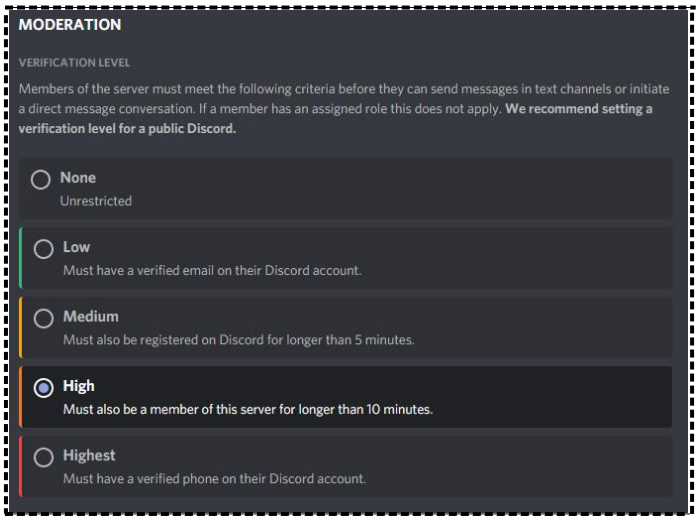
Roles control what your members can and can't do on your server

7 For Those Without Roles

For when a member doesn't have a role with permissions, add a verification level

Using this will help protect your server from spammers

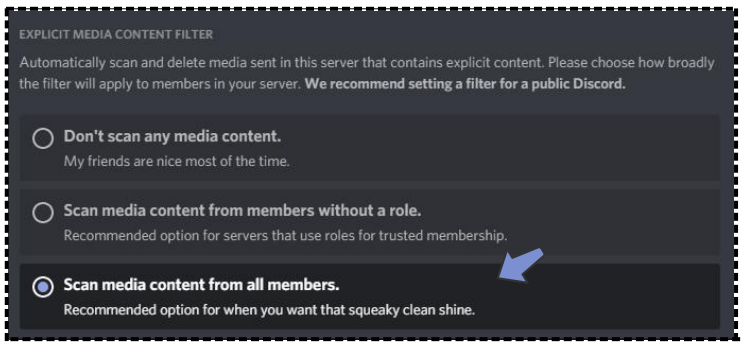
Under 'Server Settings' click on 'Moderation' and then select the appropriate level



8 Turn On Explicit Filter

Discord can automatically filter uploads and delete those that seem inappropriate

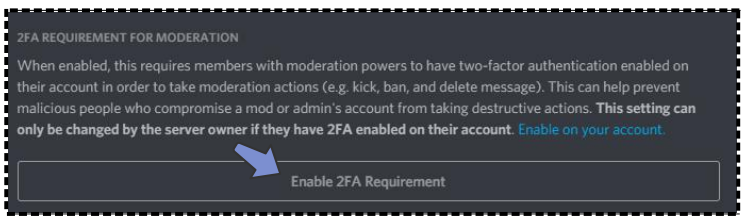
To enable this go to the 'Moderation' menu, under 'Explicit Media Content Filter', then select 'Scan media content from all members'



9 2FA for Moderation

This helps prevent people who gain access to a moderation or admin account from using it maliciously

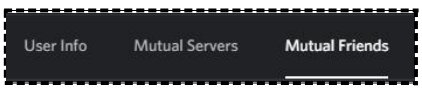
Under 'Moderation' Scroll down and there is an option '2FA Requirement for moderation'



10 Stalking Mutual Servers/Friends

Even if someone isn't friends with you, they can check whether you have mutual friends or servers with them

There isn't a way to turn this off, but keep it in mind



Social Media Privacy Settings

ON

LinkedIn

Be careful when sharing your personal information online - it could be used by others to target you

1 Settings & Privacy

Click on the 'Me' icon at the top of your LinkedIn page
Then click on 'Settings & Privacy'

2 Personal Details

Click on 'Profile information' on the left, here you can change your personal details, consider not sharing your location

Sharing your location will put you and your valuables at risk, if you show that you're away on holiday, it means your house may be vacated and someone could break in without your knowledge

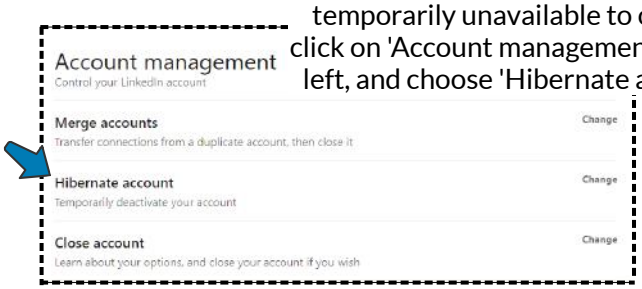
3 Profile Pictures

Consider who you want to be able to see your profile picture

Sharing this to the public will make it easier to identify you

4 Account Management

If you want to make your account temporarily unavailable to others: click on 'Account management' on the left, and choose 'Hibernate account'

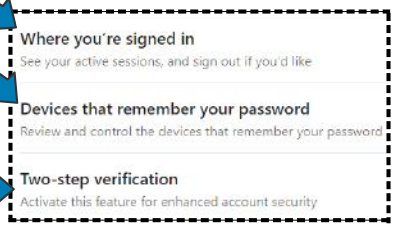


5 Sign In and Security

On the left click on 'Sign in & Security' here you can see:

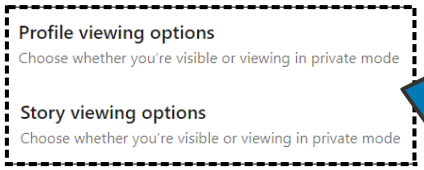
It is important to keep track of these in case someone else logs into your account!

Two-step verification is important to protect your account from others!



6 Visibility

To make it harder to be recognised, click on 'Visibility' on the left then turn on 'Anonymous LinkedIn Member'

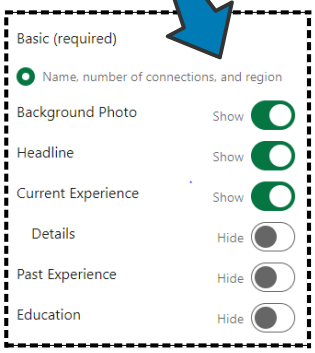


The option right under does the same but in this case it's for people's stories. This can be turned to anonymous too

This makes you anonymous when viewing other people's profile and story

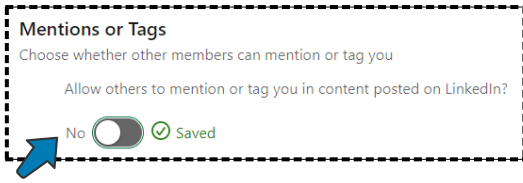
7 Public Profile

Under 'Visibility' click on 'Edit your public profile' here you can decide what you want someone who isn't your connection to see



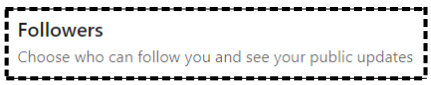
8 Mentions or Tags

To change whether people can tag you in their content or not, go to 'Visibility' and then 'Mentions or Tags' and select 'No'



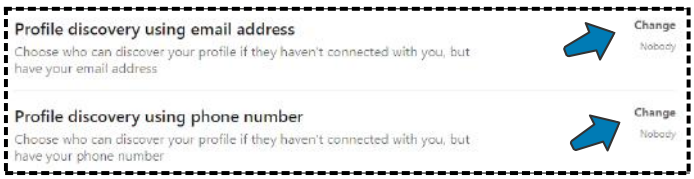
9 Followers

Under 'Visibility' click on 'Followers', here you can set whether you want those who aren't connections to be able to follow you, which will let them see your public updates



10 Profile Discovery

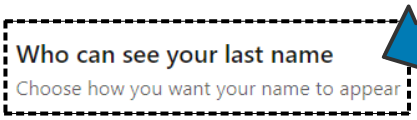
Under 'Visibility' there are two options, 'Profile discovery using email address' and 'Profile discovery using phone number', consider changing these to nobody, to make yourself less easy to be found



11 Last Name

To avoid people finding your and other accounts in your name, change your name to its abbreviated form

Under 'Visibility' click on 'Who can see your last name' this is only for those who are not a connection



Disclaimer! Anyone who is a connection will still be able to see your full name!

12 Email Address

To set your account so that others cannot see your email address:

Under 'Visibility' click on 'Who can see of download your email address'

Who can see or download your email address
Choose who can see your email address on your profile and in approved apps or download it in their data export

Set this to 'Only visible to me' and select 'No' where it asks whether to allow someone to download your email address

Only visible to me

No

13 Connections

To change your settings to stop people from viewing the people you connect with:

Change 'Who can see your connections' to 'Only you'

Who can see your connections
Choose who can see your list of connections

Who can see your connections displayed on your profile

Only you

Other members will still be able to see connections that have endorsed you or any connections they share with you. If you don't want your endorsements visible, switch your option to Only you. Learn more

14 Active Status

To change whether people can see when you're active, go to 'Manage active status' under 'Visibility' and select 'No one'

Manage active status
Choose who can see when you are on LinkedIn

Who can see that you are currently active while you are using LinkedIn?

Your Connections only
Only your 1st-degree connections will be able to see when you are on LinkedIn.

All LinkedIn members
All LinkedIn members will be able to see when you are on LinkedIn.

No one
No LinkedIn member will be able to see when you are on LinkedIn, and you will not be able to see when others are active.

Changes to this setting may take up to 30 minutes to take effect.

15 Public Posts

Under 'Public Posts' there's an option about who can follow you, turn this to friends

Profile and Tagging
Public Posts
Blocking

There are more options on this page regarding who can do what to your public profile

This is important to consider because you don't want people you don't know commenting on your profile

16 Who Can Reach You

Under 'Communications' click on 'Invitations to connect' here you can consider who can offer to connect with you, since you need to accept the request, you don't need to change it

Who can reach you
Manage who you'd like to get communications from

Invitations to connect
Choose who can connect with you

Everyone on LinkedIn (recommended)
Only people who know your email address or appear in your "Imported Contacts" list
Only people who appear in your "Imported Contacts" list

17 Network Invitations

Invitations from your network
Choose what invitations you'd like to receive from your network

Allow your network to send you page invitations to follow companies and organizations?
On

Allow your network to send you event invitations?
On

Allow your network to send you invitations to subscribe to newsletters?
On

You can change whether or not your network can send you connections by going to the 'Communications' menu and then into the 'Invitations from your network'

18 Messages

Under 'Communications' click on 'Messages' consider who you want to allow to message you

Turn this off to avoid threatening messages from those who aren't connected

Messages
Allow select people to message you

Enable message request notifications
Yes

Allow others to send you InMail?
Yes

Allow LinkedIn partners to show you Sponsored Messages?

LinkedIn Sponsored Messages are messages from our partners with informational or promotional content that is part of a marketing or hiring campaign. Unless you choose to, your name and email address will not be disclosed to LinkedIn's marketing partners.

Yes

19 Messaging

Turning off read receipts and typing indicators can hide when you have read a message

Do this through the 'Communications' menu, by clicking on 'Messaging experience' and then 'Read receipts and typing indicators' and turning this off

Read receipts and typing indicators
Turn on read receipts and typing indicators

When messaging a connection who has it enabled, both of you will be able to see when each other is typing and when the message is read.

Off

When sending a group message, non-connections will see read receipts and typing indicators. These settings do not apply to InMail and Sponsored Messages

Sources

Log In

- To check your password strength: https://howsecureismypassword.net/
- https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/password-managers
- https://authy.com/guides/
- https://www.ncsc.gov.uk/cyberaware

Social Media

- https://www.ncsc.gov.uk/guidance/social-media-how-to-use-it-safely
- www.internetmatters.org/parental-controls/social-media/
- https://www.internetmatters.org/about-us/our-partners/facebook-internet-matters-corporate-partner/
- https://www.facebook.com/safety
- https://www.internetmatters.org/resources/whatsapp-safety-a-how-to-guide-for-parents/

Securing Your Browser

- https://www.getsafeonline.org/software/web-browsers/

Security

- https://support.apple.com/en-gb/HT203977
- https://www.androidauthority.com/backup-android-phone-708622/
- https://www.net-aware.org.uk
- https://www.internetmatters.org/resources/downloading-viruses/
- https://uk.pcmag.com/how-to/46435/how-to-take-a-screenshot-on-any-device
- https://www.ncsc.gov.uk/cyberaware/home
- https://www.getsafeonline.org/protecting-your-computer/Backups/
- https://computing.which.co.uk/hc/en-gb/articles/208270025-How-to-factory-reset-a-computer
- https://www.internetmatters.org/advice/
- https://www.internetmatters.org/parental-controls/

harbour
working for safer communities

THE BUSINESS RESILIENCE CENTRE FOR THE NORTH EAST

NERSOU
NORTH EAST REGIONAL SPECIAL OPERATIONS UNIT
Protecting communities from organised crime