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
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
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**
- 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)
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.

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

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

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

Why should you use it?

In the event your password is compromised, 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.

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

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.

1. 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

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. Extra Help

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

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. **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 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 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**

   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.

Log in to Twitter

![Login page](image)

Find your Twitter account

Enter your email, phone number or username:

![Find account page](image)

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.

How do you want to reset your account?

We found the following information associated with your account.

- Text a code to my phone ending in 22
- Email a link to to**@s**********.

Continue

I don’t have access to any of these
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.

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.

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

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'.

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

 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.

SECURING YOUR BROWSER

Safari

Private Browsing

Incognito Mode

Changing Your Settings
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.

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

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

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 delete your search history and cookies when you close the browser.

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

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'.

Updates

Keep Firefox up to date for the best performance, stability, and security.

Version 96.0 (64-bit) What's new

Firefox is up to date

Show Update History... Check for updates

Allow Firefox to

- Automatically install updates (recommended)
- Check for updates but let you choose to install them

This setting will apply to all Windows accounts and Firefox profiles using this installation of Firefox.

Use a background service to install updates

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:

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'.

Updates

Keep Firefox up to date for the best performance, stability, and security.

Version 96.0 (64-bit) What's new

Firefox is up to date

Show Update History... Check for updates

Allow Firefox to

- Automatically install updates (recommended)
- Check for updates but let you choose to install them

This setting will apply to all Windows accounts and Firefox profiles using this installation of Firefox.

Use a background service to install updates

To become more efficient with updates, enable 'Automatically install updates (recommended)' by selecting the relevant circle on the left hand side.
Increase your security by using a suitable password manager rather than saving passwords to your browser.

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.

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.

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 except 'Clear history when Firefox closes'.

Securing Your Browser
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.

**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.

---

Securing Your Browser
Securing Your Browser

**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'.
Securing Your Browser

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.

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.

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.
Securing 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.

**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.

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.

WHAT CAN YOU DO?

Search yourself online

Deactivate and delete

Check your privacy settings

Review your profiles

Think before you post

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

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

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

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.

MANAGING THE RISKS

Report content

Photo location

Keep personal details private

Turn off GPS

Information leaks

Moving address

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.

HOW DO YOU KNOW IF THERE IS MALWARE ON YOUR DEVICE?
Watch out for these signs:

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

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

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.

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

How to backup on Apple Devices

Set strong passwords for your backups.

How to backup on Android Devices

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

Security
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.
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.*

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

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

Digital Resilience Toolkit

These skills will constantly be evolving and changing as technology does.

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.

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.

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

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

Advice by Age?

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.

Lots of games have age ratings to help you out.

General Guides and Resources?

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.

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.

Lots of games have age requirements for a reason.

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 are free to download, but include in-game purchases.
Information about online issues?

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

Setting Controls?

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

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

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

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

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

Can be an icon

Occasionally require secondary software

Some require a ‘Parent/Master’ account

Occasionally require setup details, relevant buttons or related web pages

Some providers automatically set

Requirements: account and relevant details, phone number
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'.

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

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'.

5. **Unrecognised Login Alerts**
   - Turn this on to receive a notification if anyone logs in from a device or browser you don’t really use.
   - In 'Security and Login', under 'Setting Up Extra Security' select 'Get alerts about unrecognized logins'.

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.

---

Social Media Privacy Settings

**Text Message (SMS)**
- Use text message (SMS) to receive verification codes. For your protection, phone numbers used for two-factor authentication can’t be used to reset your password when two-factor is on.

**Select a Security Method**
- **Authentication App**
  - Recommended - use an app like Google Authenticator. Your phone must be unlocked to generate verification codes for more protection.
  - Use Authentication App

**Unrecognised Login Alerts**
- When you’re logged in, you can check what devices are logged into your account, and log out of any if necessary.

---

Privacy: Terms - Advertising - Ad Choices - Cookies - More - Facebook © 2021
The less information you share, the less criminals will know about you, making it harder for them to attack you!

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.

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.

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.

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.

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.

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
Social Media Privacy Settings

**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.

---

Be careful when sharing your personal information online - it could be used by others to target you.
Social Media Privacy Settings on TikTok

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.

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

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.

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

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.

1. **Social Media Privacy Settings**
2. **Instagram**
3. **Settings**
4. **Privacy**
5. **Stories, Guides and Activity Status**
### 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.

1. **Security**
   - Login security
   - Password
   - Login activity
   - Saved login information
   - Two-factor authentication
   - Emails from Instagram

2. **Two-factor authentication**
   - Choose your security method
   - Authentication app (recommended)
   - We'll check to see if you have one. If you don't, we'll recommend one to download.
   - Text message
   - We'll send a code to the number you choose.

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

1. **Similar Account Suggestions**
   - Include your account when recommending similar accounts people might want to follow.

2. **Submit**
   - Temporarily disable my account

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

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

1. First search for and view their account

2. **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**.
Be careful when sharing your personal information online - it could be used by others to target you.

Social Media Privacy Settings on Snapchat

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.

   Snapchat uses the following permissions while you're using the app:
   - Camera: Use your camera to take Snaps, video chat, add friends by Snapcode, and more.
   - Contacts: Your contacts will be uploaded to Snapchat's servers so that you and others can find friends and to improve your experience. Find out more in our Privacy Policy.
   - Location: Snapchat uses your location for features like Filters, Search, Snap Map, advertising and more.
   - Microphone: Use your microphone to record audio for video chat, and more.
   - Storage: Save Snaps and Stories to your device's photo gallery, load and save app settings and cache content and more. We also use this permission to detect screenshots.
   - Phone: Autofill your phone number when you register Snapchat and adjust audio automatically.
   - Call Log: Check calling phone number to verify your identity in activation.

    PRIVACY
    - Clear Conversation
    - Clear Search History
    - Clear Top Locations
Support

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

Privacy
Privacy settings
Remove and block friends
Download my data
When does Snapchat delete Snap Chats?
Advertising and interest preferences
Learn about our service providers
I have a privacy question
Your privacy at Snapchat, explained

Social Media Privacy Settings

10 Privacy Questions

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

Contact us
How can we help?
• My account login
• My Snapchat isn’t working
• My Snapstreaks have disappeared
• I have a Filters or Lenses question
• I have a business concern
• I have a Spectacles question
• I have a Bitmoji question
• I have a Snap Store question
• Report a safety concern
• I have feedback
• I have a privacy question

Privacy Questions

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

If it’s a privacy concern, there is a Snapchat Support site

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

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

Important!

If you experience harassment, bullying or any other safety concern, you can always report it to us. Together we can make Snapchat a safer place and a stronger community.

To report a Story on Snapchat, just press and hold on the offending Snap until a report Snap button appears. Tap it to report the Story and let us know what’s going on.

To report a Snap someone sent you, just press and hold on the Snap until a report Snap button appears. Tap it to report the Snap and let us know what’s going on.

To report a Snapchat account, press and hold on that Snapchat user’s name and tap the @ button. Tap “Report” to report the account and let us know what’s going on.

To report a Story on the web, click the button on the video, then click “Report”. To report a Story on the web from your phone or tablet, tap the button on the video to report it and let us know what’s going on.

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

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

**Social Media Privacy Settings**

**Twitter**

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'.

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.

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

Activating multiple authentication methods is possible. A tick will verify if that method has been activated.
5 Control Your Direct Messages

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

3 Blocking Accounts

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

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.

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.

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

Social Media Privacy Settings
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**
   - 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.
   - Showing profile photos: choose to show or hide profile photos of other members.

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!
   - Two-step verification: Activate this feature for enhanced account security.

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.

7. **Public Profile**
   - Edit your public profile:
     - Choose how your profile appears to non-logged in members via search.
   - Under 'Visibility' click on 'Edit your public profile' here you can decide what you want someone who isn’t your connection to see.

8. **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.

9. **Last Name**
   - 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.

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.

**Social Media Privacy Settings**
To set your account so that others cannot see your email address:

Under 'Visibility' click on 'Who can see of download your email address' and set this to 'Only visible to me' and select 'No' where it asks whether to allow someone to download your email address.

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

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

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

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.

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'.

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.

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.

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

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