HEDDLU DE CYMRU
SOUTH WALES POLICE

Comisiynydd yr Heddlu a Throseddu De Cymru
South Wales Police and Crime Commissioner

Cyberstalking & Harassment Guidance

South Wales Police

2025

Mae'r ddogfen hon hefyd ar gael yn Gymraeg.

This document is also available in Welsh.

Cyberstalking is repeated and deliberate use of the internet and other electronic communication tools to engage in persistent, unwanted communication intended to frighten, intimidate or harass someone.

The guidance given in this booklet contains up-to-date information from January 2025. This booklet should be reviewed and updated the following year in January 2026. If there is any information that becomes outdated, then please refer to the subjects help centre, which can be searched for online.

Additionally, this booklet contains the possible methods used by an offender of Cyberstalking and Harassment. This does not mean that all the methods mentioned will apply to your circumstances but, will help you to prevent the possible use of these methods being used by the offender in the future.

You should also be aware that by removing the technological stalking methods being utilised by the offender, that there is an increased risk of them carrying out their actions in person as an alternative.

Paladin
National Stalking Advocacy Service
www.paladinservice.co.uk

National Stalking Helpline
Suzy Lamplugh Trust
www.suzylamplugh.org/Pages/Category/national-stalking-helpline

Protection Against Stalking
Look Forward Not Behind
www.protectionagainststalking.org

Reporting an Incident

When reading this document, you or someone you know may be experiencing Cyberstalking and Harassment. It is important to let the correct services know in order to safeguard yourself and others.

If it is not an emergency

If it is not an emergency, you can report:

- online
- by calling 101
- by going to a police station

Is it an emergency?

Does it feel like the situation could get heated or violent very soon? Is someone in immediate danger? Do you need support right away? If so, please call 999 now.

If you have a hearing or speech impairment, use our textphone service 18000 or text us on 999 if you've pre-registered with the emergencySMS service.

Help and support

Cyber Aware
Advice on protecting yourself online
www.ncsc.gov.uk/cyberaware/home

National Cyber Security Centre
Help on improving your online security
www.ncsc.gov.uk

Refuge
Advice for women and children against domestic violence
https://refugetechsafety.org

Revenge Porn Helpline
Information and help one on getting online images removed
https://revengepornhelpline.org.uk

Domestic Abuse Support
Visit our website for a list of national and local organisations
www.south-wales.police.uk/advice/advice-and-information/daa/domestic-abuse/support-organisations/

Contents

Foreword

Chloe Williams, Cyber Graduate

During my time in university, I majored in Cyber security. It was necessary for me to complete a dissertation, which I decided would be concerning the impact of social engineering on our society. Looking back, I did not connect the dots between social engineering and stalking and harassment. However, from working on Project Athena, I was able to look through a different lens. I recognise now, that social engineering can be used as one of many methods for much more wrongful purposes.

I was encouraged to undertake this project by Detective Inspector Andrew Westlake, who emphasised the impact of Violence Against Women and Girls (VAWG) on our society, and on our forces too. Speaking to our force Stalking Co-Ordinator, it was clear that through the enhancement of technology, comes an unfortunate development in the way offenders can digitally stalk and harass their survivors. My line manager further encouraged this project and proposed to focus on guidance that can be given to officers, staff and survivors surrounding Cyberstalking and Harassment.

The Child Sexual Abuse and Exploitation (CSAE) analyst network (2024) found that stalking and harassment accounts for 85% of all online and tech-enabled offences. This is a massive concern not only for our society, but for all police forces throughout the country and one which South Wales Police takes very seriously.

When working on Project Athena, I was able to speak to a survivor of VAWG. Through her bravery of speaking about the personal experiences she has faced, and still does, brought this subject very much to reality for me. Hearing about the way this survivor carries out her daily life, due to the actions of the offender, was truly saddening. Her experience has been a key factor of my motivation, and I hope that however small, this project will help survivors of Cyberstalking and Harassment, welcome back normality into their lives.

By completing Project Athena, I hope to raise awareness of the methods used by offenders in Cyberstalking and Harassment. Additionally, I hope that it will provide knowledge to officers, staff and survivors, of ways to ensure the security of devices and mitigate these offences from happening.

Introduction

Violence Against Women and Girls (VAWG) reached a climax in public consciousness following a series of stranger attacks on women by men with the most devastating of consequences.

Notably the murders in June 2020 of Bibaa Henry and Nicole Smallman who had been hosting a birthday picnic a park in London, the kidnap, rape and murder of Sarah Everard in March 2021 by a then serving police officer and Sabina Nessa murdered in September that same year in south London, who like Sarah, was simply walking home.

These are the most abhorrent of cases, and sadly VAWG proliferates through many other crimes including domestic abuse, stalking, harassment, coercive and controlling behaviour, assault and exploitation, to name but a few.

Women and girls are disproportionately affected, and such is the concern of this offending, the UK sought to place Violence Against Women and Girls on a par with Terrorism, making it a national threat as part of the Strategic Policing Requirement (SPR).

> **“VAWG crimes describes behaviours which are committed primarily, although not exclusively, by men against women. It includes incidents related to domestic abuse including controlling or coercive behaviour, rape and other sexual offences, stalking, harassment, so called ‘honour’ based abuse, forced marriage, female genital mutilation, child sexual abuse, modern slavery and human trafficking focusing on sexual exploitation, prostitution, pornography and obscenity”**
>
> (Crown Prosecution Service, 2019)

The National Picture

From the National Policing Statement 2024 for Violence Against Women and Girls we know that;

- At least 1 in every 12 women will be a survivor of VAWG per year (2 million survivors) – although this is expected to be higher, due to offending being underreported
- Between April 2022 to March 2023 VAWG offending equated to just under 20% of all police recorded crime
- Five key high harm threats have been identified namely; sexual violence, domestic abuse, stalking, Child Sexual Abuse and Exploitation (CSAE), and online and tech-enabled VAWG
- In the year ending March 2023, police recorded: 103,135 rape and serious sexual offences, 400,213 domestic abuse-related crimes, 436,196 stalking and harassment offences and from August 2022 - July 2023, 41,540 CSAE offences were committed against girls aged 10-17.
- The evolving threat posed by Online and tech-enabled VAWG showed August 2022 - July 2023 there were at least 123,515 VAWG offences which had an online element
- Stalking and harassment accounted for 85% of all online and tech-enabled offences.

Tech-enabled and facilitated offending became elevated in the consciousness of Policing UK, with the conviction of a former police officer in 2023, who facilitated the sexual abuse and blackmail of hundreds of young females on-line, receiving an unprecedented life sentence tariff.

We know with the evolution in smart technology, homes, vehicles and devices all have tracking capability, and surveillance can be carried out remotely often without detection, if robust access controls are not in place.

Violence Against Women and Girls – The Strategic Policing Requirement and National Framework for Delivery

Being part of the Strategic Policing Requirement (SPR), Violence Against Women and Girls has a 4P plan, with the key drivers of Pursue, Prepare, Protect and Prevent, which operates alongside the National Framework for Delivery.

South Wales Police has its own action plan, aligned to the same priorities, which in summary;

Pursue:

We are responsible for pursuing VAWG offenders as they cause significant harm and often offend repeatedly.

We must target our resources to pursue the highest harm and repeat offenders - related to our five key threats.

Protect:

We have a statutory duty to protect and safeguard survivors of VAWG

We must enhance our approach to protect survivors of VAWG - recognising the balance required between timely enforcement and meeting wider survivors needs.

Strategic Policing Requirement

National Framework for Delivery

Prepare:

A fundamental requirement to effectively pursuing VAWG offenders is to ensure we have the right capabilities, capacity and culture

We must prioritise the professionalisation and specialism of our workforce, with the effective use of resources, whilst not undermining our operational requirements.

We commit to improving our response to online and tech-enabled VAWG, through;

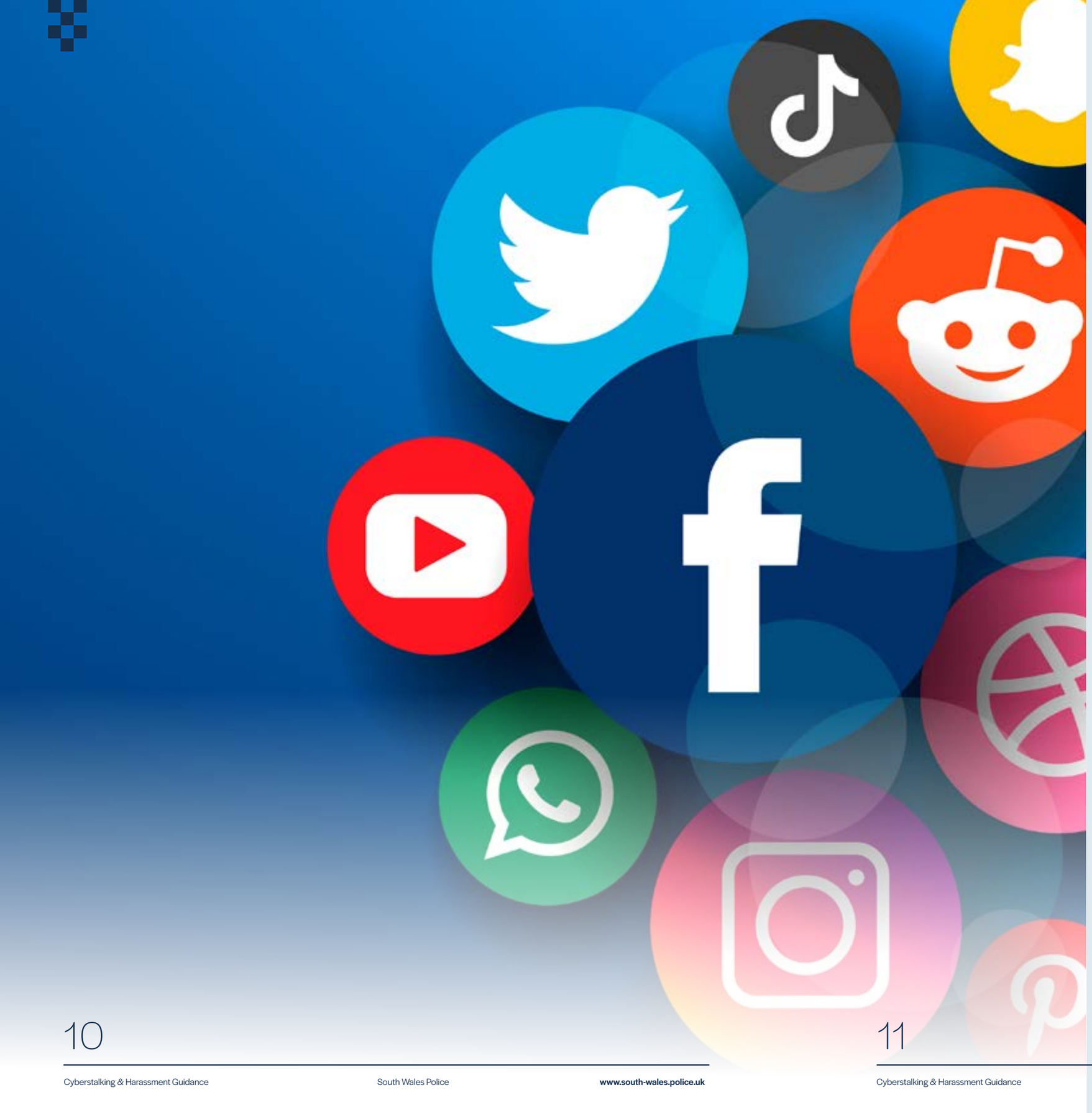
- providing a tailored response to online harm to protect survivors of all ages
- recognising, understanding, and being prepared to respond to the threat of generative artificial intelligence (the threat this poses to young people)
- sufficient dedicated resources and specialist training and recruitment
- encouraging the government to strengthen regulation to effectively deter and prevent the ongoing proliferation of VAWG online.

Prevent:

We are clear on our role within a whole-system approach to prevent VAWG

We must have a coordinated partnership response to VAWG with a focus on early prevention within which we will play our role.

South Wales Police and the Police and Crime Commissioner have stated their on-going commitment to tackling Violence Against Women and Girls.



Part One:

Guidance for Social Media Accounts

Interactions among people in which they create, share and/or exchange information in virtual communities & networks.

Facebook & Instagram (both owned by Meta)

Instagram - a photo and video sharing app that allows you to send messages to friends.

Facebook - allows you to send messages and post status updates to stay connected with family and friends.

The offender will use Facebook & Instagram to:

Gain information from your profile - for example, they could look at your posts to see who you are spending time with (photos of you with friends or family).

Comment on everything you post - these comments could be abusive/ threatening.

Use the messaging features - for example, continuously bombarding you with messages throughout the day.

Tag or mention you in posts - they could Tag or Mention you in an inappropriate post that all your followers will be able to see.

Logging into your account - if the offender has access to your account, they could post inappropriate content on your profile. They could also read your messages and/or message your friends and family pretending to be you.

Try and locate you - if you have moved away from the offender, they can look at your profile to see if the content gives away where you are located (such as the town).

Many people will use Facebook, Instagram or both. The guidance given below applies for both platforms.

Blocking people

Block the offender and any other accounts they may have. You should also check through your 'followers'/ 'friends' list, any people following you that is linked to the offender should be removed.

Go to the profile of the person you want to block > click on the three dots (...) > tap 'Block'.

Privacy settings

Check your privacy settings and configure your account to be private; by having a private account you will have approval on who can follow/be friends with you.

Create a private account

Instagram - click the more icon at the top right of your profile > tap on 'Account privacy' > Tap on the toggle next to 'Private account'.

Facebook - tap on 'Menu' with your profile picture in the bottom right corner > tap on the settings icon at the top right corner > scroll down to 'Audience and visibility' and tap on 'Followers and public content' > next to 'Who can follow me' select 'friends'.

Turn off your activity status

This will prevent accounts that follow you to see when you were last active online:

Instagram - click the more icon at the top right of your profile > scroll down to 'How others can Interact with you' and tap on 'Messages and story replies' > tap 'Show activity status' > ensure the toggle is turned off.

Facebook - tap on 'Menu' with your profile picture in the bottom right corner > tap on the settings icon at the top right corner > scroll down to 'Audience and visibility' and tap on 'Active status' > ensure the toggle is turned off.

Message controls

Decide whether message requests go to your chat list, your "Message requests" folder, or whether you receive them at all:

Instagram - click the more icon at the top right of your profile > scroll down to 'How others can Interact with you' and tap on 'Messages and story replies' > tap 'Message controls' > tap 'Others on Instagram' > ensure 'Don't receive requests' is marked.

Facebook - go onto the Messenger app > tap on 'Privacy & Safety' > under 'who can reach you' tap 'Message delivery' > tap 'Others on Messenger or Facebook' > ensure 'Don't receive requests' is ticked.

Tags and mentions

Choose who can tag you in their photos and reels, and who can @mention you to link your account in their stories, posts etc.

Instagram - click the more icon at the top right of your profile > scroll down to 'How others can Interact with you' and tap on 'Tags and Mentions' > under 'who can tag you' tap 'don't allow tags or toggle 'Manually approve tags and toggle 'Don't allow mentions.'

Facebook - tap on 'Menu' with your profile picture in the bottom right corner > tap on the settings icon at the top right corner > scroll down to 'Audience and visibility' and tap on 'Profile and tagging' > for 'who can see what others post on your profile?' select 'only me' from the drop-down menu. For the 'Tagging' section, both should be set to 'Only me'. Additionally, both toggles should be enabled in the 'Reviewing' section.

> **Note -** This will ensure that you can review any tagged photos before they are posted. This is to protect your location as many people will tag the place on their posts, or the background of the photo may easily show where you are.

Personal information

Remove any personal information on your social media.

Remove search engines from linking your profile

Instagram - to stop search engines linking your Instagram profile, you must request through their Help/Support webpages.

Facebook - tap on 'Menu' with your profile picture in the bottom right corner > tap on the settings icon at the top right corner > scroll down to 'Audience and visibility' and tap on 'How people can find and contact you' > ensure the 'Do you want search engines outside Facebook to link to your profile' toggle is disabled.

If you believe the offender has/ or can access your Instagram/ Facebook account

Change your passwords and set two-factor authentication (2FA).

Change your passwords

Instagram - click the more icon at the top right of your profile page> scroll down to 'privacy centre' and tap on it (this will take you to the Meta centre, where both your Facebook and Instagram accounts should be) > tap on the more icon which is at the top right corner > tap on 'Manage your accounts' > under 'Account settings' tap 'Password and security' > tap 'Change password' > select the account you want to change the password of.

Facebook - click on the menu tab at the bottom right corner > tap on the settings icon at the top right corner > 'Meta accounts centre' will be shown at the top, tap on it > tap on 'Password and security' > 'Change password'.

Set two-factor authentication

Instead of tapping 'change password' when following the steps above, you will find 'Two-factor authentication' below it to tap on instead.

Review your linked devices and login history

If evidence is found that someone else has been accessing your account, a screenshot should be taken:

Instagram - click the more icon at the top right of your profile page> scroll down to 'privacy centre' and tap on it (this will take you to the Meta centre, where both your Facebook and Instagram accounts should be) > tap on the more icon which is at the top right corner > tap on 'Manage your accounts' > under 'Account settings' tap 'Password and security' > Tap 'Where you're logged in' > check both Instagram and Facebook accounts by tapping on them.

If you see an unrecognised device > tap on 'Select device to log out'

Facebook - click on the menu tab at the bottom right corner > tap on the settings icon at the top right corner > 'Meta accounts centre' will be shown at the top, tap on it > tap on 'Password and security' > from here, the following steps are the same as above.

> **Note -** you can also receive login alerts by tapping on 'Login alerts' that comes under 'Where you're logged in.
>
> You should check that the recovery details are your own- this can be done by taking the same steps as mentioned above, but instead of tapping 'Password and security' you tap 'Personal details' instead. This will tell you what email addresses and phone numbers are linked to your account. You can delete an email or phone number by tapping on them and then 'delete email' or 'delete number'.

X (formerly known as Twitter)

A news and social networking site where people communicate in short messages.

The offender will use X to:

Use the messaging features - for example, continuously bombarding you with abusive messages throughout the day.

Tag or mention you in posts - they could Tag or Mention you in an inappropriate post that all your followers will be able to see.

Comment on everything you post - these comments could be abusive/ threatening.

Logging into your account - if the offender has access to your account, they could post inappropriate content on your profile. They could also read your messages and/or message your friends and family pretending to be you.

Mute and block

Go onto the 'X' app > search for the person you wish to block or mute and tap on their profile > tap on the three dots located at the top right corner of their profile > tap on either 'Mute @ [profilename]' or 'Block @[profilename].

Note - for the best outcome, blocking the offender is strongly advised.

Audience and tagging

Protect your posts

This will only show your posts to people who follow you. You will need to approve each new follower:

Tap on your profile picture located at the top left corner of the home page > tap on 'settings and privacy' > tap on 'Privacy and safety' > tap on 'Audience and tagging' > ensure the 'Protect your posts' toggle is enabled.

Photo tagging

When photo tagging is turned off, people will not be able to tag you in photos:

These are the same steps as 'protect your posts' with an extra step. When tapping on 'Audience and tagging' tap on 'photo tagging' > ensure the toggle is turned off.

Direct messaging

You can decide who can message you by going onto the direct messaging settings. If you have blocked the offender, then you will not receive any messages from them. If someone follows you, they will always be able to message you:

Tap on your profile picture located at the top left corner of the home page > tap on 'settings and privacy' > tap on 'Privacy and safety' > tap on 'Direct messages' > under 'Allow message requests from:' select 'No one'. This will mean that even if the offender sends you a message using a different/unblocked account, you will not receive it.

You can also manage/review what devices have access to your direct messaging -

Tap on your profile picture located at the top left corner of the home page > tap on 'settings and privacy' > tap on 'Privacy and safety' > tap on 'Direct messages' > tap 'Manage encrypted devices' > if any devices are unrecognised, tap the 'X' icon next to the device to remove it.

Discoverability and contacts

You can control your discoverability and manage contacts by:

Tap on your profile picture located at the top left corner of the home page > tap on 'settings and privacy' > 'Privacy and safety' > tap on 'Discoverability and contacts' > ensure that the toggles in these settings are all disabled.

Change your password and set two-factor authentication (2FA).

Guidance on how to create strong passwords and set up 2FA can be found on page 32.

Tap on your profile picture located at the top left corner of the home page > tap on 'settings and privacy' > 'Your account' > tap 'Change your password'.

Tap on your profile picture located at the top left corner of the home page > tap on 'settings and privacy' > 'security and account access' > 'Security' > tap on 'Two-factor authentication'.

Note - in 'Your account' you can also see the email address linked to your account by tapping on 'Account information'.

Apps and sessions

You can see information about when you logged into your account by:

Tap on your profile picture located at the top left corner of the home page > tap on 'settings and privacy' > 'security and account access' > 'Apps and sessions' > here you will see 'sessions', 'Account access history' and 'logged-in devices and apps.

WhatsApp

An instant messaging and video calling app.

The offender will use WhatsApp to:

Harass you - for example, continuously bombarding you with abusive messages throughout the day.

Logging into your account - if the offender has access to your account, they could read your messages and/or message your friends and family pretending to be you.

Find your location - the offender may have set up your account to share your location with them

Blocking someone

Open WhatsApp > go to 'Settings' > tap on 'Privacy' > 'Blocked' > tap on 'add new' and type in the number you wish to block.

Report the offender

WhatsApp will receive the last five messages sent to you by the reported user, and the user won't be notified).

Open WhatsApp > click on the offenders profile > scroll down and tap 'Report [name]'.

Linked devices

You can link other devices to your account, including Windows, Mac and Web).

Open WhatsApp > go to 'Settings' > tap 'Linked devices' > if any devices are linked to your account they will be shown. If there are any you do not recognise > tap the device > log out.

Privacy settings

Profile photo

You can choose who gets to view your profile photo

Open WhatsApp > go to 'Settings' > tap 'Privacy' > 'Profile photo' > choose between which setting you would like to be configured by tapping on it.

Groups

You can choose who is able to add you to groups. Instead of tapping on 'Profile photo', tap on 'Groups' instead. Choose between the different settings presented by tapping on it.

Live location

You can check to what chats you are sharing your location with

Open WhatsApp > go to 'Settings' > tap 'Privacy' > 'Live location' > if you are sharing your location with someone else, disable it.

Chat lock

If there are chats that you want to hide.

Tap on the contacts profile photo > scroll down and find 'Lock chat', tap on the toggle to turn it on. You can unlock these chats by using your phone passcode, Face ID, fingerprint or with a secret code.

Two-factor authentication (2FA)

You can set up 2FA to add an extra layer of security.

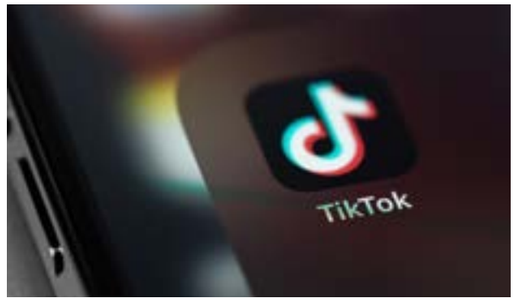
Open WhatsApp > go to 'Settings' > tap 'Account' and then 'Two-step authentication'

Protecting IP address on calls

To make it harder for someone to infer your location, calls on your device will be securely relayed through WhatsApp servers.

Open WhatsApp > go to 'Settings' > tap 'Privacy' > scroll down and tap on 'Advanced' > enable the toggle for 'Protect IP address in calls.

Note - There is no way to hide your phone number when using WhatsApp.



TikTok

A platform used for creating and sharing short videos.

The offender will use TikTok to:

Harass you - for example, continuously bombarding you with abusive messages throughout the day.

Logging into your account - if the offender has access to your account, they could post inappropriate content on your profile. They could also read your messages and/or message your friends and family pretending to be you.

Look at what content you're posting - for example, they could look at your posts to see who you are spending time with (photos of you with friends or family).

Try and locate you - if you have moved away from the offender, they can look at your profile to see if the content gives away where you are located (such as the town).

Blocking someone

Find the user's profile > tap the three dots in the top-right corner > tap on 'Block'.

Make your account private

This means that only people that follow you can watch your videos, LIVE videos, bios and likes.

Tap the profile icon in the bottom right > open the menu in the top right > Settings and privacy > Private account.

You can enable TikTok to stop suggesting your account

Go to your profile > Open the menu in the top right > Settings and privacy > Suggest your account to others > Switch off the toggles of your choice.

Turn location services off

Tap the profile icon in the bottom right > open the menu in the top right > Setting and privacy > Privacy > tap Location services > turn off location permissions.

Direct messaging

To change who can send you direct messages.

Go to your profile > Open the menu in the top right > Settings and privacy > Privacy > tap Direct messages > out of the options, choose 'friends'. Any followers that you follow back can send you a direct message.

Create a strong and unique password

Tap on 'Profile' at the bottom > tap the Menu button at the top > 'Settings and privacy' > tap 'Account' and then tap 'Password'.

Enable two-factor authentication

Tap the profile icon in the bottom right > open the menu in the top right > Setting and privacy > tap Security > tap '2-step verification' and choose at least two verification methods.

Snapchat

An app that lets you send pictures or videos, called “snaps” that vanish after viewing; there is also a chat function.

The offender will use Snapchat to:

Harass you - for example, continuously bombarding you with abusive/threatening messages or videos throughout the day.

Logging into your account - if the offender has access to your account, they could see who you have been snapchatting and/or message your friends pretending to be you. They could also post inappropriate content on your Snap Story.

Look at what content you’re posting - for example, they could look at your stories to see who you are spending time with (photos of you with friends or family).

Try and locate you - If Ghost Most is disabled then they could be locating you via your Snap Maps.

Blocking someone

Click on your avatar in the top left corner > scroll down your friends list and locate the person you want to block > hold down on their name > tap ‘Manage friendship’ and select ‘Block’.

Ensure that that you only have friends and family on your Snapchat

Click on your avatar in the top left corner > scroll down your friends list and check to see if there is anyone you do not recognise or are close with > to remove someone, hold down on their name > tap ‘Manage friendship’ and select ‘Remove Friend’.

Put yourself in ghost mode

To protect your location, ensure that the maps feature is turned off.

Click the map icon in the left-hand corner > tap on the setting icon in the right-hand corner > ensure that the toggle for ‘Ghost Mode’ is enabled.

To only allow a certain group of friends to view your stories

Click on your avatar in the top left corner > under ‘My Stories’ click the three dots by ‘Add to my Story . Friends only’ > tap on ‘Story Settings’ > customise who you want to view your story by tapping on ‘Custom’.

Ensure your password is strong and unique

Click the map icon in the left-hand corner > tap on the setting icon in the right-hand corner > tap on ‘Password’ and change your password.

Ensure two-factor authentication

Click the map icon in the left-hand corner > tap on the setting icon in the right-hand corner > tap on ‘Two-Factor authentication’ and tap ‘Continue’.

Pseudonyms

Used by a person to conceal their identity.

In some cases, once the offender knows the name of your social media profiles, they will continuously bombard you with friend and message requests. Even when you block one account, they will create another in its place, this can become draining having to report and block endless accounts.

Offenders will try to contact you on any sort of online account if it's possible to. This could include finding your profile on gaming platforms or on dating apps.

If this is happening to you, then you should consider using pseudonyms for your online accounts. Using a pseudonym will make it much harder for the offender to find you online (if at all), and you will be able to use your accounts without being flooded with fake friend requests and messages.

Additionally, if you do use a pseudonym then the profile picture should not be of you, or anything that could identify to the offender that it is you.

Only family and friends you trust should know about these accounts. The more people you allow to follow you, the greater the chance of it possibly getting back to the offender.

Doxing

Publicly providing personally identifiable information about an individual via the internet and without their permission.

Offenders will gather as much personal and private information about you. They can gather this information via the internet, third parties (e.g. mutual friends), and, if the offender is not blocked by you, they can also find out information from your social media.

This information can be used to build up a profile of you, which the offender will post online with the purpose of harassing, intimidating, or harming you (e.g. posting where you live or private medical records). Facebook, Twitter, and Instagram are popular social media platforms that the offender can use to post about you.

In cases where you are being doxed by the offender, Google offers a feature where an individual can request to remove select personal identifiable information (PII) from Google Search results. For example:

- Address, phone number, email.
- Confidential ID numbers (social security, Tax ID etc)
- Bank account/ credit card number.
- Highly personal, restricted, and official records (e.g. medical records)

Request content removal from Google Search results

Google also offers an individual to create a 'Google alert'. You can receive emails when new results for a topic show up in Google search, this includes getting information about mentions of your name. This can be done by -

Go to Google Alerts > enter the name you want to follow/look for > click 'Show options' > change the settings according to your preference (e.g. how often you get notifications, how many results you want to see etc.)

If you are alerted of personal information about you being posted online- then you can send in a content removal request (guidance above).

Additionally, if the offender has been posting personal information on social media- then yourself or a third party (in cases where the offender is blocked) should report the post/ account via the platform.

Impersonation/fake accounts

An impersonation account on social media is a profile that falsely represents a person, entity, or organisation.

The offender may create fake social media accounts of you and claim them to be a 'new' account. Offenders may create fake accounts of you for a few reasons, the most common motives will be:

Reputational Damage - offenders may impersonate you to spread false information about you, which could harm your reputation and cause you distress.

Trick third parties - offenders could trick your friends and family into connecting with the impersonated account. This could be to gain information about you, or, to create conflict between third parties and yourself.

Note - offenders could also create fake accounts of third parties to get to you.

To mitigate possible impersonation accounts and their success, it's important to understand one of the vital techniques an offender will use:

- **Social engineering** - this is the manipulation of individuals into revealing sensitive information or performing actions that will compromise the security of the survivor. An offender will manipulate emotions by creating a sense of urgency, fear, or sympathy. In cases where you and offender were once in a relationship, this is particularly a risk. This is because they will know personal things about you, making it easier to pass off and impersonate you.

Because of this, it's important that yourself and third parties can detect fake accounts, the red flags are:

- **Low follower count and engagement** - fake profiles will often have a low number of followers and limited engagement on their posts. It should also be considered who the profile follows, such as if the account only follows your family and friends.
- **Profile information & photos** - check for discrepancies of the profile. If you have blocked the offender for some time, then the photos and information used on the fake profile will be outdated.
- **Activity and interaction** - a true/real social media account is usually alive with interactions, if the profile seems static with no interactions its usually a red flag that the account is fake.
- **Suspicious posts** - the offender may share content that seems out of character for the person they are pretending to be.
- **Unusual communication** - it's important to stay cautious of unsolicited messages. This is especially if the account is asking for information, money or trying to direct you to suspicious links.
- **Language and communication style** - it's important to consider how the account is communicating with you. Is the account using the same style of messaging as the real person would or is it different? Are they talking to you in an unusual way or a way that could be considered out of character for the real person.
- **Is the 'old' social media account still active** - if it is a fake account, then the legitimate person will still be using their original/real account.

The offender may create an account impersonating you, one of your family members, or a friend.

If any third parties/or yourself are not sure if the account is real or fake, then -

- Ask about the account on a communication platform that you know is secure and is the true person. This could be over text message, or to be sure, you should ring the individual or ask them in person.

Note - You should also take caution if you believe an account communicating with you to be fake. Additionally, you should be careful about what information you share over social media platforms and be wary of any suspicious links a suspected account share with you.

If an account is known to be fake, it's important to take the right action as soon as possible:

- **Gather evidence** - yourself and third parties should take screenshots/capture relevant information that proves the existence of the fake profile. This includes posts, messages, and interactions.
- **Report the impersonator** - yourself and third parties should report the account to the social media platform by using their reporting tools (include the evidence you gathered).
- **Notify your network** - you should inform third parties about the impersonation account. This is to prevent them from communicating with the fake account and possibly sharing information. This should be shared as a public post on the platform, private messages or in person.
- **Monitor** - Yourself and third parties should stay alert for new impersonation accounts and report any new activity promptly to the platform.
- **Review and update security measures** - you should ensure that your security features are up to date on social media accounts (guidance given on pervious pages).

Part Two:

Guidance for Mobile Phones (Apple & Android)

Emails

A system of sending and receiving messages via digital devices over a network.

Hate mail and threats could be composed by the offender and can be sent through a burner account (email set up temporarily to not divulge their primary email address) or remailer (provides anonymity). It is also important to note that malware can be sent through an email by attaching a malicious link. This type of malware could be spyware between third parties and yourself.

If hate mail or threats via email is being sent to you -

- You should create a new folder in your email account of all the offenders offensive/ harassing emails. This way you have evidence if needed in the future.
- Block the email address.
- Report the messages to the email service provider
- In some cases, an offender may even get a hold of your work email. In this case, your employer should be made aware of the circumstances.
- Consider using different email addresses for different purposes.
- Create a filter; this is a set of rules that tells your email service how to handle certain emails. A filter can automatically delete emails from a particular sender or that moves all emails with certain keywords to a specific folder
- If applicable, ask third parties to block the offenders email.

Note - It is crucial for you to change your password of your email account. This is probably the most important account for you to ensure stays protected. All our accounts are linked to our email, and if we forget our password for an account, we can reset it by sending password recovery to our email. If the offender can access your emails, it will open the doors for them to access your other accounts and possibly lock you out of them by resetting the passwords. Not only that, but confidential and personal information can also be found on our email accounts.

Mobile number and voicemail

Mobile number - A set of figures that identifies a mobile phone subscriber- used to make calls and text messages.

Voicemail - Allows people to leave a recorded message when the recipient is unable to answer the phone.

Offenders can use your mobile number to bombard you with messages throughout the day, these messages are often, but not always, threatening and abusive. They can also attempt to ring you throughout the day, and if they can't get through, will leave voicemails.

Note - Your voicemail greeting should ideally be set to the default one, rather than your voice. If the offender was unsure if it was your number, rang it, and it went to voicemail, the default greeting would not give away it is you.

You should block the offenders number on your mobile -

iPhone - Settings > scroll down and tap on 'Phone' > scroll down and tap on 'Blocked contacts' > tap on 'Add New...'

- If you have an iPhone and a MacBook, then you will need to block the offender on both devices. (IOS and MacOS are two different systems)

Android - open messages > tap the more icon in the upper right-hand corner > settings > tap 'Block numbers and spam' > tap 'Block numbers.

If you share children with one another and there needs to be a point of contact, you could consider using a trusted third party as point on contact.

If the offender uses another number or multiple numbers after their main number has been blocked, then you can block the unsaved number. You can do this by using the same steps as above and entering the number manually rather than by the name of the contact.

Ask third parties to block the offenders number if possible.

When you block a mobile number from your phone, voicemails can still be left from the offender.

- There are apps that can allow you not only to block unwanted calls but their voicemails too. Call control is an app that can be downloaded from Google Play Store and Apple Store. Their integrated partners are Nextiva, Cisco and BroadSoft.

Apple ID & iCloud accounts

Apple ID is a user account by Apple for their devices and software, contain the user's personal data and settings.

iCloud is the service from Apple that securely stores your data in the cloud and keeps it up to date across all your devices automatically.

In cases where you and offender were once in a relationship, the offender may have created an apple ID/iCloud account for you that they are also linked to. The offender could even configure your apple ID/iCloud so that they have access without you even knowing.

If an offender has access to/or shared the same Apple ID/iCloud as you then they can see your downloads, purchases, messages, photos, videos and contacts. Call logs will also be shared between the two phones. The offender can also find out your location.

Settings > tap on the name > scroll down and check devices linked to the account - Any devices that are not recognised by the user should be removed.

Sign-in & security > email & phone numbers - The email addresses and phone numbers listed can be used to sign in. Check to see if there are any unrecognised emails or numbers linked, if so, remove.

Family sharing > check to see if this has been set up - If so, check to see what users are shown and remove any that are not recognised.

Settings > messages > send and receive - Check to see which email addresses and phone numbers can send and receive messages.

Safety check > review all the personal and security information in your account to see if there is any information that someone else has added.

- You could also disable iCloud sync on your device, this means that data from your device will no longer be stored online and cannot be accessed by anyone who may have access to the iCloud account.
- You could also enable advanced data protection for iCloud, this is the highest level of cloud data security whereby it is protected by end-to-end encryption.

Signing in to the Apple ID website can allow a user to review all the personal and security information in their account to see if there is any information that someone else has added.

Setting up two-factor authentication for Apple ID is highly advised- even if someone knows the password, they will not be able to access the account without the pin.

Android accounts

The Android operating system was developed by Google. To access email, contacts, and calendar, and to get apps from the Google Play Store, a Google account must be created, information associated with that account syncs with the phone.

In cases where you and offender were once in a relationship, the offender may have created a Goggle account for you that they're also linked to. The offender could even configure your Google account so that they have access without you even knowing.

If an offender has access to/or shared the same Google account as you then they can see your messages, photos, videos and contacts. Call logs will also be shared between the two phones. The offender can also find out your location. .

Android phones use a Google account. If you have an Android account, then there are a few ways in which you can check to see if another device has access to your account.

- **Google account > security > your devices > manage all devices**. This will let you see what devices are signed into your google account or were signed in recently. You can check to see what type of information that device/ session has access to via the google account.
- **Google messages app** - an offender may connect one of their devices to your messaging app and through cloud messaging.
- **Google family link** - check to see if you have Google family link installed on your phone. (This can also be used for apple users)
- You can check to see if your phone has been configured to hide apps. **Settings > Display > Home screen > Hide apps**.
- **Life360** - this is another app that can be used to track and monitor you, especially in cases where you may have left a coercive relationship.

Change password on the Google account - you should ensure that your Google account cannot be accessed by the offender (this could have been possible/likely if you and the offender were once in a relationship).

Change the password of your Google account; this is to prevent remote access. To change a Google account password:

- Settings > Google > manage your Google account > at the top, tap Security > 'How you sign in to Google' > tap Password (you might need to sign in) > Enter your new password > tap Change Password.

How to create strong passwords and two-factor authentication (2FA)

From the National Cyber Security Centre (NCSC)

If an offender knows your passwords for your accounts, and you do not have two-factor authentication enabled, then this runs the risk of them accessing your accounts at any time. As mentioned previously, offenders can access your accounts to gain information about your online activities as well as private information. The offender can use this information against you and can even use specific accounts to cause damage. For example, gaining access to your email account and writing a harmful email to your boss.

Three random words

The National Cyber Security Centre (NCSC) encourages people to use three random words as a technique to create passwords.

According to the NCSC (2024):

> **"Longstanding advice around making your passwords very complex (which suggests we should create passwords full of random characters, symbols, and numbers) is not helpful. This is because most of us have lots of passwords, and memorising lots of complex passwords is almost impossible."**

Three random words will make it very difficult for an offender to guess and a very long time for a computer to crack. Additionally, it can also be remembered much more easily.

Password manager

Having to create different passwords for all the accounts we have means that we must remember all those different passwords, a password manager can help with this. Password manager is an app that stores your passwords, so you don't need to remember them, many password managers can also enter your passwords into websites and apps automatically (so you don't have to type them in every time you log in).

There are many different Password Manager apps available, you should research into the apps before choosing one to use.

Note - some password manager apps will even generate strong passwords for you.

National Cyber Security Centre

Two-Factor Authentication (2FA)

2FA is a crucial security feature that should be implemented by everyone (especially on E-mail accounts). Even if the offender or another individual knows your passwords, they still won't be able to access your accounts if 2FA is enabled.

This works by sending a PIN or code (often by SMS or email) that you will need to enter before being able to access the account.

If 2FA is available for an account, the option to enable it is usually found in the security settings of the account.

Like Password Manager, there are third-party apps available to download that will provide the user an authentication method. Again, applications should be researched before choosing one to use.

Top tips for staying secure online
www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online

‘Find My’ & other location features (Apple)

‘Find My’ can be used on iPhone to see the location of a device on a map. If the device is online, you see its location and will play a sound to help you find it. If the device is offline, you see its location, but it doesn’t play a sound.

If an offender is linked to your ‘Find My’ or any other location feature, then they will know exactly where you are. Knowing this information can be unsafe, they could turn up to where you are, cause a scene, or even threaten/attempt to harm you.

Find my iPhone/friend - this is a feature that is popular amongst friends and family members with iPhones. It allows a person to share their location with someone for an hour, until the end of the day, or indefinitely.

You should check who you are sharing your location with on this app. If there are any unfamiliar devices linked to your location, they should be deleted. To do this -

- Find my > People > these are a list of people who are either sharing their location with you, you’re sharing your location with them, or both. To check if you’re sharing your location with that person, tap on their name > scroll down - you will either see ‘Share my location’ or ‘Stop sharing my location’. If you’re sharing your location with an unwanted device, tap ‘Stop sharing my location’.

Ensure that no third parties of the offender are linked to your location, this could be in cases where you are still in contact/meet up with friends or family of the offender.

Apple messages - in cases where you and offender still have one another’s phone numbers and use iPhones messaging as a way of contact, you should check to see if your location is being shared with them. This can be done by:

- Messages > tap the conversation thread with the person in question > tap their photo > if you’re sharing your location, ‘Stop sharing my location’ will be shown as an option. If this is the case tap on ‘Stop sharing my location’.

Note - There are commercial apps that can be installed onto a device (such as Life360 & Google maps) that can be used to track your location. This is a likely possibility if you were once in a relationship with the offender.

Check to see what apps are installed on your phone, if you come across apps on your device that you’re unfamiliar with then you should research them on a safe/secure device. If a tracking app has been installed on your phone, then you should take screenshots and uninstall the app.

You should also check to see if you have any hidden apps on your device. One way to uncover hidden apps is to change the restrictions in your settings -

- Settings > screen time > content & privacy restrictions > apps > allow all.

Note - Hidden apps on iPhone is a feature on iOS18 and above.

Google Location (Android)

With Google Location sharing, you can choose who can find your location and how long you want to share your location.

If an offender is linked to your 'Find My' or any other location feature, then they will know exactly where you are. Knowing this information can be unsafe, they could turn up to where you are, cause a scene, or even threaten/attempt to harm you.

Find my device app

When a Google account is added to an Android device, Find My Device is automatically turned on. The devices most recent location is available to the first account activated on the device.

You can check to see you're sharing your location with and remove those devices by -

- Find My Device > Shared device > Settings > look to see who the device is sharing their location with. To remove a device, next to the person tap More > Stop sharing.
- If the offender knows your Google account details- then they can use the Find My Device app to sign in as you and locate your device (this is a feature used on the app if a device is 'lost'). It's important that you change your password to the Google account.

Google Maps location

This allows you to share your real-time location. It allows an iPhone user to track an Android user and vice versa.

Survivors should check if their location is being shared with any devices on this app, they can also remove a device by -

- Google Maps app > tap on your profile > Location sharing > check to see who the device is sharing their location with. To remove a device, tap on their profile > tap stop.

Note - There are commercial apps that can be installed onto a survivor's device (such as Life360) that can be used to track a survivor's location. This is a likely possibility if the survivor was once in a relationship with the offender.

Survivors should check to see what apps are installed on their phone, if they come across apps on their device that they are unfamiliar with then they should research them on a safe/secure device. If a tracking app has been installed on their phone, then they should uninstall the app.

- Survivors should also check to see if they have any hidden apps on their device.

Children accounts on Android and Apple

Child accounts on iPhones and Android are used by parents who want to effectively manage and safeguard their child's digital activities.

Offenders may configure your device as a child's account so they can control parts of its function. This is a form of coercive control and allows them to have influence over who you can talk to, what apps you can use, and will allow them to view your location at any given time.

This can also be used on your children's devices, when you and offender have separated but share children with one another, the offender could have set up the children's devices to be child accounts. Although this can be seen as safeguarding their children, its usually so they can abuse the features such as the location feature.

When your device/s is set up as a child account, the offender can:

- **Control talks and text** - the offender can decide which contacts you can talk to and text, and when you can talk/text them. (Note: Parental controls don't allow them to read text messages)
- **Control/view app & website activity** - this allows the offender to choose which apps/ features you can use, when and how long you can use them and view your activity on apps and websites.
- **View location** - the offender can prevent changes to certain privacy settings, including 'Share My Location' settings. This means that the offender can configure your phone to always share your location with them.

How to check if a device is configured as child account:

Apple

Open settings > Apple ID > tap Family > if it's prompting you to set up Family, then the account is not associated with a Family account. If it takes you to a set up family account, tap on your name.

Here you will see if the device is set up as child's account, there are a few ways to know this:

- The age of the account is set between 13 and 17.
- There are devices linked to the 'Parents/ Guardian' section.
- Location sharing section is sharing the device's location with other named devices.

If a device is set up with a child account, then it may be possible to leave family sharing. If the account is aged between 13 and 17, a device can leave Family Sharing if the 'parent' or 'guardian' hasn't turned on Screen time for the devices account. If they have, then the device can't leave the group without permission from the organiser.

Android

- You can check to see if a device is part of Family link by looking at the Google account associated with the device. On the Google account, like Apple, it should say the age of the person linked to the Google account.
- Additionally, if you head over to the Family Link app, it will open to the interface where you can view what 'members' are part of the group your Google account it linked to.

If the Google account is a child's account under the age of 13, then the 'parent' or 'guardian' will have to allow permission for the account to leave Family link.

For both Apple and Android devices, there is a possibility that they may be able to factory reset the device. However, Apple and Android have features that even if factory reset takes place, the device cannot be used with another Apple ID or Google account. This is a feature used in cases where a device may have been stolen or to prevent bypassing child supervision.

Spyware

Stalkerware, which is also referred to as spyware, refers to a type of app or software that is designed to be hidden from the owner of a device. This allows someone to spy on activity, track their location, or even record keystrokes.

Offenders may install spyware onto your device. This is so they can monitor you through your phone. For example, they can watch anything within view of your phone camera and even access your microphone.

In cases where the offender is an ex-partner, there is a possibility that they have planted stalker ware/spyware onto your devices.

Some common signs that you may have spyware on your device:

- Performance issues - spyware is constantly working hard in the background of a device and retrieving a person's data, this is why your device may be running slower than usual.
- Battery life draining unusually quick - tracking a device through spyware and gathering data from the device can cause your phone to drain its battery quickly.

You can check to see which apps are using your battery by:

iPhone & Android: Settings > Battery > Battery usage by app. You can check to see if there are any suspicious/unknown apps using your battery usage.

- Phones temperature suddenly rising - its normal for the temperature of a phone to increase when its charging or using an app for a long period of time, however, it shouldn't happen when your phone is inactive or doing light tasks.
- The phone turns on & off randomly.

It should be noted that these signs should be considered, however, it does not necessarily mean there is 100% spyware on your phone (there could be other innocent reasons for it).

Check the apps that you have installed on your phone. It should be noted that spyware can be masked as another app (e.g. calculator app, diary etc.) You should remove any apps that are unfamiliar.

If you have been or are in a situation where you suspect stalkerware/spyware is likely to have been installed on your device- then factory reset can be advised. This is because there are spyware apps that will not be displayed like a normal app (Backing up important data should be undertaken).

Hidden app features on iPhone and Android -

- You should be made aware that iOS18 now allows you to hide apps. One way to uncover hidden apps is to change the restrictions in their settings:
- Settings > screen time > content & privacy restrictions > apps > allow all.
- Another way of uncovering hidden apps is through looking at purchased apps in the app store.

You should also check to see your Android phone has been configured to hide apps. Settings > Display > Home screen > Hide apps.

If you find an app that you want to uninstall:

iPhone

Look through the phones home screen and find the app you want to delete > tap and hold on to the app > select 'Remove app' > confirm by hitting 'Delete app'.

Android

Settings > Apps > tap on 'see all apps' > find the app you want to delete > tap on 'Uninstall' > tap 'ok'.

Emergency services configuration

With emergency SOS, you can quickly and easily call for help and alert your emergency contacts.

If an offender is locating where you are or is following you, then Emergency services can be configured on your phone. This is for instances where you feel unsafe leaving your home, the offender is physically following you, and/or is showing aggressive/threatening behaviour.

Note - On iPhone 14 and above, you can use satellite to text emergency services when you're off the grid with no cellular and Wi-Fi coverage. You can try the demo by settings > Emergency SOS > scroll down to 'Emergency SOS via satellite' and tap 'Try Demo'.

Quickly call emergency services:

iPhone

- Simultaneously press and hold the side button and either volume button until the sliders appear and the countdown on Emergency SOS ends > release the buttons.
- Another way to enable an iPhone to start Emergency SOS is by quickly pressing the side button five times -
  - Settings > Emergency SOS > tun on 'Call with 5 Presses'

When an emergency call ends, your phone will alert your emergency contacts with also your current location- they will also receive updates when your location changes.

To add emergency contacts

- Open the Health app > tap on your profile > Tap Medical ID > Edit > scroll to Emergency Contacts > tap the add button > tap on the contact > add their relationship.
- Call Quietly (available on iOS 16.3 and later) - when Call Quietly is turned on and you try to make an emergency call, any warning alarms and flashes will be silenced.

To enable this -

- Settings > Emergency SOS > Turn on 'Call quietly'.

Android

- Settings > Safety and Emergency (may be in Advanced features) > Emergency SOS.
  - When this is turned on, you can quickly press the side key (usually the power button) five times.
- You can also configure your device to send a message to your emergency contacts. Messages will include location information, an audio recording from your phone's microphone, a written request for help, and a warning if your phone is almost out of battery.

This can be done by -

- Settings > Safety and Emergency > 'Share info with Emergency contacts' > Choose which contacts you want to notify if Emergency SOS is enabled.

Linked devices

AirPods/Earpods

Portable speakers that fit inside people's ears and connect to any audio-producing device using Bluetooth audio technology.

An offender can use AirPods and other wireless Earpods to monitor and locate where you are.

Note - You may not be aware that you have AirPods, or another type of location enabled Earpods around you (Offenders could have put them in your bag, pockets etc). It is advised for you to check your bags and pockets, especially in cases where you and offender once had/or still do have a relationship.

You can locate AirPods and other wireless Earpods (e.g. Beats) with an iOS device using Apple's Find My app, and features such as 'Lost Mode' and 'Family Sharing'.

- Family Sharing - allows you to share your AirPods location with family members. This means that an offender could be connected to your AirPods and can track your location. You can check to see who is connected to your AirPods by going on to 'Find my' > Devices or People. Remove any devices that are unrecognisable or unwanted.
- Even if AirPods are switched off or dead, there is a 'Lost Mode' to find them. Marking them as 'lost' alerts you if they are connected to another iOS device, the 'finder's' location and lets you send a custom message. Only the owner with the owner account can activate this, so if the AirPods were gifted by the offender- then this is something to consider.
- If the AirPods were given to you by the offender, then the AirPods will have to be reset, and this can only be done by the owner. It is advised that if you still have/use the AirPods, you should dispose of them.

Smartwatches

A smartwatch is a portable device worn on the wrist that supports apps and acts as an extension of your mobile phone.

An offender can use smartwatches to monitor and locate where you are.

Apple watch

the same as AirPods, an Apple watch may be set up on 'Family Sharing' which allows any device on that feature to track and locate where the Apple watch is. You should check if your apple watch is connected to 'Family Sharing' mode, and if so, what devices are you allowing to locate the watch.

- Settings > [your name] > if you see 'set up family sharing', you're not using Family sharing with that Apple ID OR if you see an icon with Family sharing, you can tap on it to see the members and roles. Then click remove on the member's name.

Note - If you are not the 'organiser' of the family sharing group but are an 'adult member' you can tap on your name > stop using family sharing.

Location can also be shared on 'Find My', an offender could have set this up on your Apple Watch. To stop sharing your location, tap the 'friend's' name on the 'Find People' screen > then tap Stop Sharing.

Like AirPods, if the watch was given to you by the offender and is set up using their account with activation lock enabled, the watch cannot be disconnected without the offenders Apple ID and password. In this case, it is advised that you dispose of the watch.

Garmin smartwatches

Garmin LiveTrack is a tracking function that allows an individual to share their real-time location and tracking information with who they choose. It works when tracking an activity, such as a run or cycle, but also when they're just wearing your watch as normal.

- You can check if LiveTrack is enabled by going onto the Garmin connect app on your phone. Select more (bottom right) > Safety & Tracking or LiveTrack > Select LiveTrack > Select the three dots (top right) > Select LiveTrack Data & Privacy > If LiveTrack is enabled, Select Opt Out.

Note - There are other smartwatches that have location/tracking features. If you own a smartwatch, you should check the configurations of the paired app. Guidance on how the location/tracking features work can be found online.

AirTags & Chipolo

AirTags and Chipolo (as well as other tags) communicate with smartphones using Bluetooth – these are used to track the location of items.

An offender can use smart tags to monitor and locate where you are.

Smart tags

Smart tags are a widely used method of tracking and locating survivors, these trackers can differ in size, shape and colour depending on the makes (some are even as small as a coin).

If the offender is locating where you are and it's not clear how, it may be possible that they have planted a tracker. These trackers can be put in bags, purses, coat pockets, inside cars etc.

It's important for you to check your clothing and bags, especially when you are heading out of the house.

You should also check your children (if applicable) the offender may have planted tracking devices in toys, bags, clothes of the child.

AirTags

Before Apple introduced new security features to help prevent involuntary tracking, AirTags were being widely used by people to track and locate where someone was.

How you can know if an AirTag is tracking you? - to help know if an AirTag is tracking you, the persons iPhone will notify you when an unknown AirTag is travelling with you. When you tap on the notification, a map will show when the unknown AirTag was first detected traveling with you.

There is even a 'play sound' feature, which will activate a beeping noise, allowing you to find the AirTag more easily.

If you have an Android device instead of Apple, then Apple advise for people to download 'Tracker Detect'. This is an application that helps Android users to discover AirTags and other 'Find My' compatible devices that are near them.

If you find an unknown AirTag, then you can stop the owner finding you by pushing down and twisting counterclockwise on the back of the AirTag > take cover off and remove the battery.

Note - This does not mean that the new safety features are 100% reliable, you should still check to make sure of AirTags.

Chipolo (best for Android)

One product of Chipolo is called a 'Card Point' which slips into a wallet and can easily go unnoticed, this uses Google's 'Find My Device' feature and is only available for Android devices.

If you find one of these card points, you can > Locate the button the bottom left corner of the device > press and hold the button for about 30 seconds and it will begin beeping in 1-second intervals > release the button after the 10th beep > when the device is disabled, there will be a conformation sound.

Note - There are many different makes of smart tags that can be used by the offender. If you find a tracker on or around you, you should find somewhere safe and in public to disable it by following the instructions on their website.

Part Three:

Guidance for Online Apps

An app is defined as a self-contained software package that allows users to perform specific tasks on a mobile or desktop device.

Online banking

Online banking allows you to conduct financial transactions via the Internet. Online banking offers customers almost every service traditionally available through a local branch including deposits, transfers, and online bill payments.

Offenders can send transactions to your bank account and contain messages (often abusive) in the payment reference field. Additionally, if they have access to your online banking app, then they can review your transactions and where these transactions have taken place. This means they can review where you have been or where you are.

If you once shared your card details or have your card details saved on the offenders phone, then applying for a new bank card is advised. This is to prevent the offender from using your bank details.

Even if you have applied for a new card or have your new card, the offender is still able to send transactions to your bank account. This can be an issue (particularly if child maintenance is involved), as offenders have been reported to misuse the payment system, by containing abusive words and messages in the payment reference field.

For those who have had a relationship with the offender, they may not have had control over their own money or banking. Fortunately, many banks now have signed up to UK Finances Financial Abuse Code of Practise (a voluntary code of practice aimed at supporting survivors of financial abuse).

Note - The banks should be able to block a particular account from leaving a message in the reference field of your account. This is particularly useful when the offender needs to send over child maintenance. Additionally, if there is no reason for the offender to be sending you money, then banks should be able to block transactions from the offenders account.

The below image shows all the banks that have signed up to the financial abuse code. If you are with one of these banks, head over to the 'Financial Abuse' support page on the bank's website. On the webpage you will find the contact information to help you with the issues you're facing relating to your bank account.

Lloyds
www.lloydsbank.com

HSBC
www.hsbc.co.uk

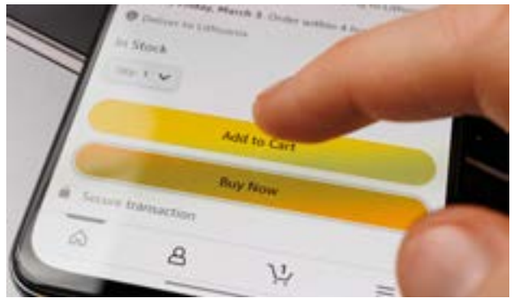
Barclays
www.barclays.co.uk

Halifax
www.halifax.co.uk

Nationwide
www.nationwide.co.uk

NatWest
www.natwest.com

Santander
www.santander.co.uk



Shopping & takeaway apps

Shopping accounts – Buying goods or services over the internet.

Takeaway accounts - Platform for buying groceries, foods from restaurants and other services.

Why is it important to ensure these accounts are secure?

Bank details - If your bank card details are saved to the account, the offender can use the card to make purchases.

Home address - if the offender still has access to the account, they will be able to see your home address.

You should review the different online shopping and takeaway accounts you have and change the account details. In some circumstances, you survivor and offender may have used the same shopping and takeaway accounts, there are a couple of things to do if this is the case:

Change the password of the account - if your email address is linked to the shopping account (the email used to set up the account) then you should change the password to be strong and secure.

Also ensure that two-factor authentication (2FA) is enabled if possible. This is to further prevent unauthorised access even if someone has the password.

Note - Changing the password and enabling 2FA can be found in the settings section of the account.

Create a new account - if the email address linked to the account is the offenders, erase all your personal details from the account, sign out of the account and create a new one.

Note - For the account to stay protected, the email address used for these accounts should also be secure. This is because if the offender has access to the email, then they can use password recovery and change the password back.

Dating apps

An online dating service presented through a mobile phone application.

Offenders can monitor dating apps to see if you have a profile, they can use your profile as a way of gaining information. For example, if you have moved away from the offender, then they can see where you have set your location to (town or city). They could also set up a fake account to 'match' with your profile and talk to you (this is a form of catfishing).

For more information visit Digital Breakup

https://refugetechsafety.org/digitalbreakup/dating-apps

There are many safety precautions to be mindful of when using dating apps. For instance, Refuge Tech Safety (2024) suggest:

- If you are on dating apps, then you should ensure that the information you share is limited in terms of personal identifiable information.
- You should also ensure that your dating profile is not linked to your social media, this is to prevent giving away more information about yourself.
- When it comes to the location feature of dating apps, set it manually and adjust it somewhere which is not specific to your location. When it comes to the photos you upload to the app, ensure that there are no photos containing third parties. This is to prevent the offender gaining information about them by possibly finding their social media accounts. You should also ensure that the photos you do post do not give anything away (such as your location).
- Be cautious with profiles you are communicating with, (such as reverse image searching their pictures) this is to check if the profile is genuine or not.
- Keep contact with the profiles on the dating app rather than move away from it for communication.
- Ensure that your security settings are adjusted and that you set up security measures such as 2FA, also use an email account separate to your regular one.

It should also be noted that on certain dating platforms you are able to block certain profiles from finding you on the app by entering a phone number of the ex/offender.

Transport apps

Uber - A platform for requesting and providing rides, meals, and deliveries.

Trainline - A platform to book train and coach tickets.

It's imperative for you to ensure that the offender does not have access to accounts such as Uber or Trainline. This is because the offender can review your detailed trip history and possibly pick up patterns of your day-to-day travel and where you may be at certain times.

Like shopping and takeaway apps, you should review the transport accounts that you have/use. If you shared the same transport accounts with the offender, then there are a couple of things to consider:

- Change the password of the account - if your email address is linked to the transport account (the email was used to set up the account) then change the password to be strong and secure.
- Also ensure that two-factor authentication (2FA) is enabled if possible. This is to further prevent unauthorised access even if someone has the password.

Note - Changing the password and enabling 2FA can be found in the settings section of the account.

Create a new account - if the email address linked to the account is the offenders, erase all your personal details, sign out and create a new account.

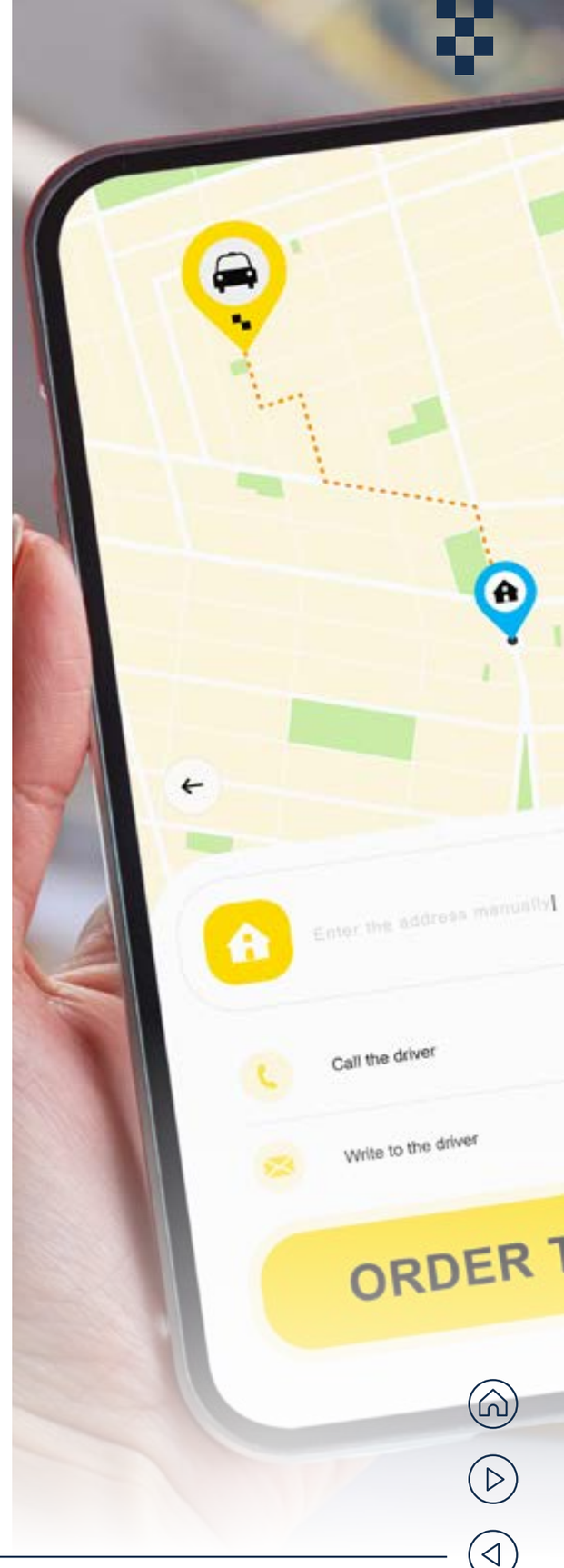
Note - For the account to stay protected, the email address used for these accounts should also be secure. This is because if the offender has access to the email, then they can use password recovery and change the password back.

Uber

On Uber, there is a feature that allows more than one 'rider'. To remove a rider:

Open Uber app > navigate to 'Riders' section > here you will be able to see all the riders that you have added to the account, look for the rider you want to delete and tap on their name > you should then see an option to delete/remove the rider from your account.

Note - When you delete a rider from your Uber account, their data is removed from your account, and they will no longer have access to your account for requesting rides



Running apps (Strava)

Track health and performance metrics. It also gives a place to store information about your workouts, running and other activities.

Offenders can use these apps to monitor your running routes and view map visibility. If you haven't configured your map visibility to mask the start and end of your route, then there is a change the offender can pinpoint where you live.

Note - Activities set to "Followers" and "Only You" will not be eligible for public segment leaderboards and may not be eligible for some challenges or achievements.

Running and similar fitness apps are becoming more popular, so ensuring that you have the correct privacy controls in place is essential for your safety. Offenders could use these apps to gather information about you.

Strava (2024), for example, have shared information on how it allows another user to see several details about someone's profile if privacy controls haven't been enabled:

Profile page

If profile privacy controls are not set to "followers" and are instead set to "Everyone", it means that the entire Strava community can see your full profile details. When the profile is to "followers" people must request to follow the profile. Ensure that the only people that follow you are family & friends and details on your account is limited. To change profile settings:

- Strava app > open settings from the icon in the upper right corner of the 'You' tab > tap 'Privacy controls' > select 'Profile page' > choose followers.

Activities

Your activity page displays data about your activity on Strava (e.g., data & time, maps (location) etc.). If the offender can see this data, then they can figure out your running patterns (e.g. what time of the day you run) and the routes you take. Ensure that your activity settings are either set to "followers" or "only you", this can be done by:

- Strava app > open settings from the icon in the upper right corner of the 'You' tab > tap 'Privacy controls' > under 'Activities', select either 'followers' or 'only you'.

Group activities

A group activity is one of your activities that has been grouped with one or more other activities by a different athlete. When you set this privacy setting to 'followers', non-followers:

- Cannot see you grouped to their activities.
- Cannot see you were part of another athlete's group.
- Cannot see you were grouped with other athletes on your own activities.

Ensure that group activity settings are either set to "followers" or for extra precaution "no one", this can be done by:

- Strava app > open settings from the icon in the upper right corner of the 'You' tab > tap 'Privacy controls' > under 'Group activities', select either 'followers' or 'no one'.

Flyby

This is a Strava Labs tool that lets you play back your activity, as well as those near you, on a map and timeline. There are two options for this setting, "Everyone" or "No one", if it set to "Everyone" all Strava athletes:

- Will be able to see if you crossed paths or were nearby on Flyby.
- Will be able to click your Flyby avatar to open your Strava activity.

Ensure that Flyby settings are set to "No one", this can be done by:

- Strava app > open settings from the icon in the upper right corner of the 'You' tab > tap 'Privacy controls' > under 'Flybys', select 'no one'.

Map visibility

This will allow you to hide portions of your activity map from other Strava athletes. There is also an option to set a default preference so that your activities automatically upload with this preference. With map visibility features, you can customize how much of the start or end of an activity is hidden up to a 1-mile radius or hide the entire map. To do this:

- Strava app > open settings from the icon in the upper right corner of the 'You' tab > tap 'Privacy controls' > tap on 'Edit map visibility'.

Blocking an athlete

If you wish to block an athlete, you can do this by:

- Open the app > from the profile of the athlete you'd like to block, tap the three-dot icon > select 'Block this Athlete'.

To view more privacy controls visit Strava
https://support.strava.com/hc/en-us/articles/207343930-Privacy-Controls

Note - You should also consider other fitness apps you may use and find out the privacy features you can set. You can do this by visiting the fitness app website, or by looking at the privacy settings on the app.

Car connected apps

Offers the ability to manage your vehicle from your phone and send remote commands.

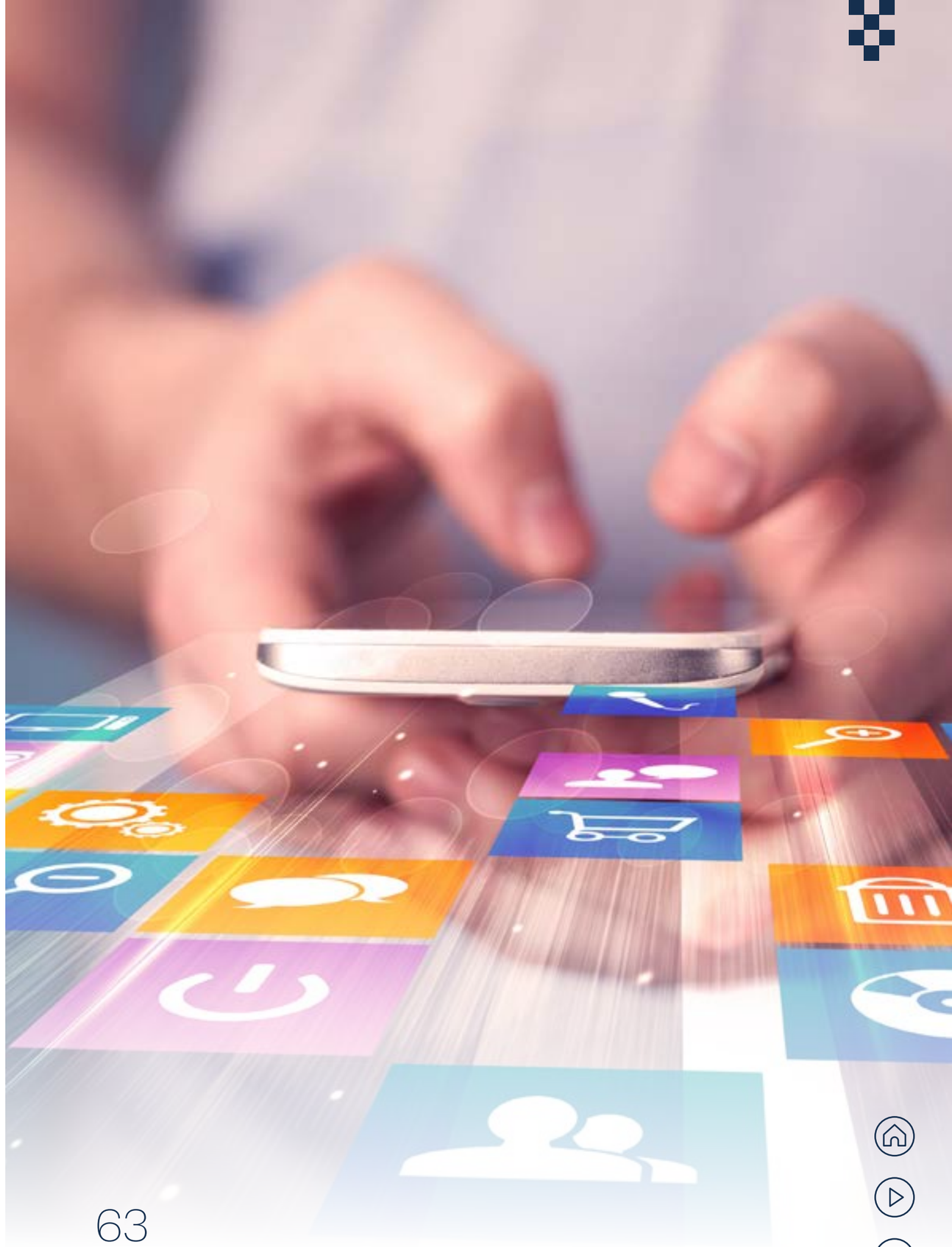
Offenders could have access to the connected app for your car. They can use this app to track where the car is located, as well as using the lock/unlock feature to gain physical access.

Note - You can attempt to revoke an apps access to their car by finding the master reset key found in settings, finding the manual for the car will explain how to do this.

Specific makes of cars now have an app that allows the owner to have a connected smartphone app. These apps allow the owner to lock/unlock a vehicle, vehicle location, remote start/stop etc.

In instances where you use this type of app, you should change the login details to the account that connects to the car. There are connected smartphone apps that allow more than one person to have access to the same car, this can be an issue in terms of location and physically accessing the car. You should ensure the only device linked to their car is your own.

- FordPass - you can have multiple users on FordPass, all users need is a Vehicle Identification Number (VIN) and enter it into their app. To remove a user a connectivity reset can be performed or a master reset.
- Remote connect (Toyota) - this allows for a car owner to see where their vehicle was last parked. The app allows the assigned user to authorize another driver to use Remote connect with their vehicle. To remove a user from accessing Remote Control > 'Remove Driver' on the main vehicle dashboard app.
- BMW, Audi, Volvo, Mini, Volkswagen and many more cars now offer connected smartphone apps that allow a person connected to locate their vehicle. This is something to be considered when dealing with cases where you and the offender had/have a relationship.



Part Four:

Guidance for Online Entertainment

Various forms of content, such as movies, TV shows, music, games, and live streams over the internet.

Gaming

Playing an electronic video game, often done on a gaming console, PC, or smartphone.

Offenders can contact you, or your children (if applicable) through gaming platforms. Often offenders will use the children you share with one another to get to you, this poses a potential risk with games that provide an online chat room. The offender could potentially create a fake account and attempt to speak to you or your children (a form of catfishing).

If you like gaming or have children that like gaming, then you should secure them to ensure an offender cannot have a point of contact or gain any personal information by having access to the account/s.

- If you shared gaming accounts or had your gaming accounts set up by the offender, then you should create new ones. The email used for the new accounts should ideally be a new email created specifically for gaming- separate to their personal account.
- When creating a password for the new gaming account, ensure that 2FA is enabled also. You should also ensure that recovery details are linked to you.
- To prevent the offender from finding your child through online gaming, the accounts name and picture should not be able to be linked back to you.

Note - There are configurations a parent can make where a child's account can be restricted from voice chat, sending, and receiving messages.

In cases where you have children who game, then parental settings are advised to be set up. Parental settings may have been set up by the offender before, in this instance, factory reset may need to be considered especially when new accounts need to be made.

Streaming accounts (Netflix, Disney+, Amazon Prime etc)

Services that offer a wide variety of TV shows, movies, documentaries and more on internet-connected devices.

The offender can use streaming platforms to leave you messages, this is done by editing the 'Who's watching?' names of the profile. Additionally, the offender can also gain personal information about you, such as email, phone number and billing details.

If the account is set up with your email address, then ensure that you change the password and log out all devices from the account. Guidance is given below:

Amazon Prime video

You can keep this account secure by:

- **Reset & use a strong and unique password** - your Prime Video account is linked to your Amazon account. You must ensure that you change the password of your Amazon account to secure Prime video. This can be done by heading over to Amazon > in the top right corner hover over 'Accounts & Lists' and tap on 'Account' > tap on 'Login & Security' > sign into your account > this should take you onto the 'Login & Security' page, by the right of 'Password' tap on 'Edit' > enter a strong and secure password.
- **Set up two-factor authentication** - follow the same steps as above up until 'Password', instead, tap 'Advanced Security Settings' > tap 'Get started' by the right-hand side of 'Two-Step Verification'.

Remove unrecognised devices from your amazon account - to remove devices from your Amazon account, head over to Amazon > in the top right corner hover over 'Accounts & Lists' and tap on 'Content and Device' > log into your account > tap 'Devices' > select the unrecognised devices and tap on 'Deregister'.

Netflix

You can keep your account secure by:

- **Reset & use a strong and unique password** - you can change your password from your account page, or you can send yourself a password reset email or text message.
- To add, change or delete a phone number from your account, go to the 'Change phone number' page > follow the instructions to confirm your identity. You can then add, edit or delete a phone number.
- **Sign out of unused or unrecognised devices** - you can either sign out of all devices or sign out of specific unused or unrecognised devices from the 'Manage Access & Devices' page.

Now TV

You can keep this account secure by:

- **Reset & use a strong and unique password** - to update your password for NOW > head over to the 'Personal details' section of 'My Account' (sign in if you're not already) > scroll down to 'Security details' and select 'Reset password' > enter your email address and select 'Continue' > click on the link in your emails and reset your password.
- **Managing devices** - you cannot log out of a single device on this account. However, you can sign out of ALL devices. To do this > head over to the 'Devices' section of 'My Account' > select 'Sign out of all devices'. Note- The device you're using to sign out from will stay signed in, so you'll still see it in your device list.

Disney+

You can keep this account secure by:

- **Reset & use a strong and unique password** - to update your password on Disney+ head over to DisneyPlus.com > select 'Log in' > Enter your email address and select 'Continue' > select 'Forgot Password' > check your emails from Disney+ and enter the 6-digit verification code to verify your email > Enter your new password.
- **Managing devices** - view or log out of any devices that you do not recognise. To do this, log into Disney+ > select 'Profile' > 'Account' > under 'Access & Security' select 'Manage Devices' > Log Out of any unrecognised devices.
- Additionally you can 'Log Out' of all devices by selecting 'Access & Security' and tapping on 'Log out of everywhere' > enter the one-time password sent to the email address connected to the Disney account and tap 'Confirm' > select 'Log out' to be signed out of all sessions and apps.

For more guidance on securing your streaming platforms, head over to their support webpages.

Part Five:

Guidance for Wi-Fi Routers

Sends information from the internet to personal devices.

Ensure that your router is locked down. This is to prevent an offender from monitoring your incoming and outgoing traffic, as well as having control over the access devices linked to that Wi-Fi have.

Change your ADMIN log-in details. The steps to this are:

- You will need to know the default password to change it. This can usually be found stuck on the bottom of the router, if not there, the documentation that came with the router or the manufacturers website. (In cases where the offender has changed the default password, then you must reset the router. This is usually done by holding down the rest button for 10-15, maybe longer, or by using a pin to press the button if it is inside the router).
- Enter the IP address of the routers administrative interface in the browsers address bar. (Note - some routers disable administration through wireless connections so you may have to connect to the router via the ethernet cable).
- Enter your routers default username and password. Once signed in, look for the security settings page and change the administrator credentials. Ensure that the new password is strong and complex.
- **Ensure to check your wireless encryption** - WPA2 is the encryption standard that you will want to use, rather than the older WPA standard. WPA2 should be turned on by default, but older routers may be using the older protocol; it is worth checking to see which protocol is enabled.
- **Disable remote router access** - Remote router access allows anyone not directly connected to your Wi-Fi network to access the router settings. You can disable remote access under the router's admin settings (below gives guidance on how to access router settings).
- **Setting up a guest Wi-Fi network** - the main Wi-Fi network will give someone access to all the connected devices and files on the network. A guest network, however, will allow visitors to access the internet without reaching local resources. This improves security and prevents the spread on viruses that could possibly enter from a guest device. To set up a guest network:
  - **Access your routers settings** - to your router's IP address in a web browser to access its settings. (If you're unsure what the IP address is, check the back of your router or the manual)
  - **Locate the guest network settings** - Find the guest network settings in your router's admin panel.
  - **Configure the guest network** - Set up the guest network with a unique name (SSID) and password. Make sure that the SSID is different from the main network SSID, so its easily identifiable. The password should also be set strong to keep it secure (guidance on strong passwords is found on page 32.
  - **Customise the settings** - Adjust the settings for the guest network to your preference.
  - **Save and test the network** - Save your settings and test the guest network to ensure it's working properly.

Virtual Private Networks (VPNs)

Virtual private networks protect their users by encrypting their data and masking their IP addresses.

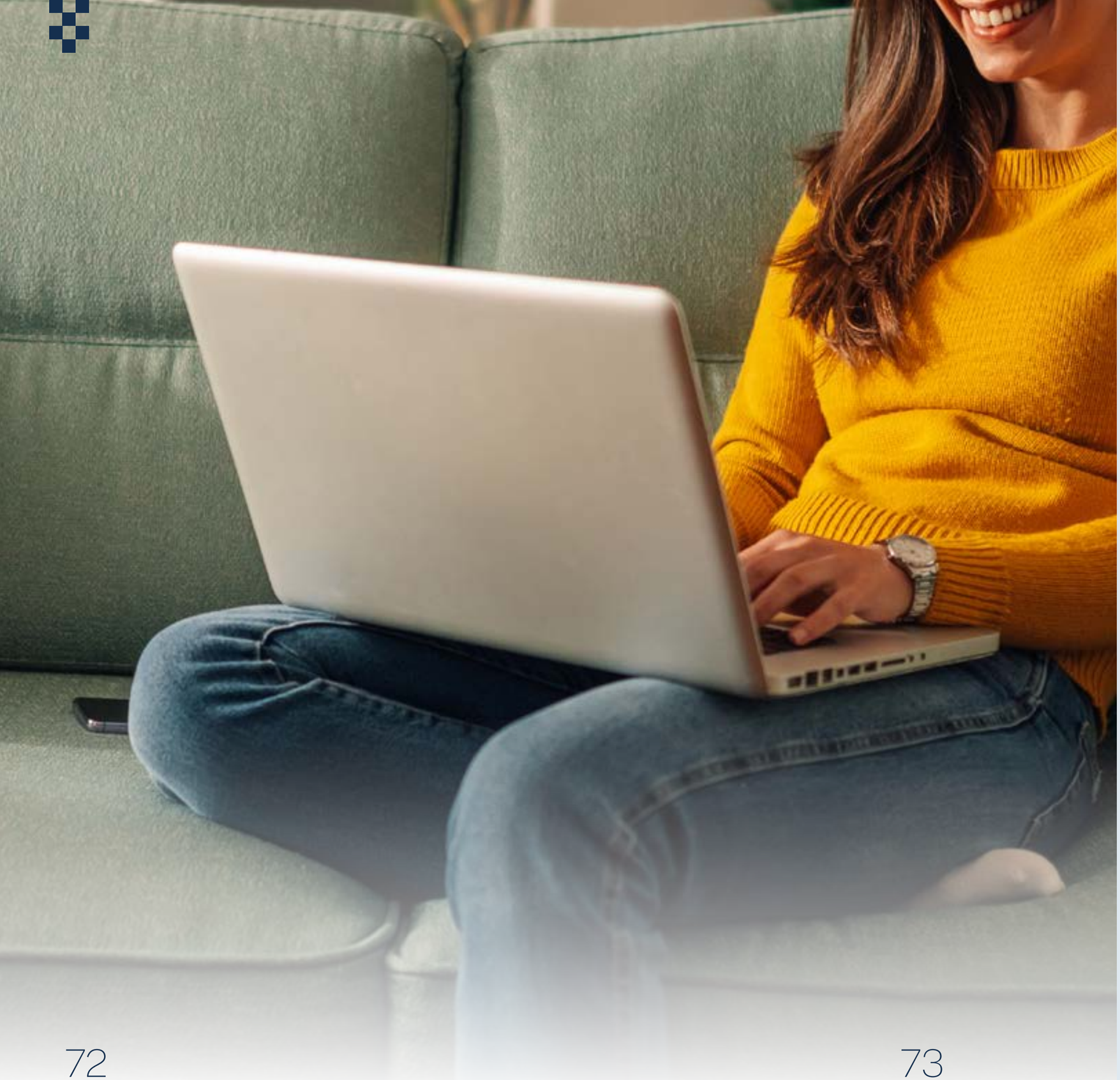
If offenders have access to your Wi-Fi router, then they can see your incoming and outgoing traffic, this a method used by them to monitor your internet activity. Additionally, all traffic is linked to an IP address, which can be used to show your geographical location (but not your exact location).

Using a VPN is a security measure that is advised to all individuals, but especially those who are survivors of cyberstalking. One of the biggest advantages you using a VPN is that it provides you with a greater level of anonymity. When you connect to a VPN, all your online traffic is routed through an encrypted tunnel - this makes it unreadable to third parties (including the offender). This means that you can use the internet privately and securely.

It works by spoofing your IP address, which means that the offender/cyberstalker only sees the IP address of the VPN server you are connected to. This masks your physical location, protecting you from the offender.

Note - VPNs can be used across all devices - this is particularly beneficial if you use more than one device (which most people do). Additionally, this adds extra security for those who have children. This means that offenders cannot gain access to information by using the children's devices, such as IP location.

You can find free versions of VPNs available online, depending on the features you want, there will also be paid monthly VPNs. Before downloading a VPN, ensure to read their specifications found on their website properly and ensure that it is a legitimate service.



Part Six:

Guidance for Laptops/Computers

Mac devices

A family of personal computers designed and marketed by Apple.

An offender can access your laptop/computer remotely or have planted malware to monitor you. They also may want to access your private files on your device, especially files that are linked to an ongoing case you have against them. Additionally, they could look for confidential files such as medical records, and even delete files.

If the offender used to have access to your laptop/computer, then there are a few things to consider as a safety precaution.

Mac Devices - it can be possible that if the offender once had access to your laptop/computer, configurations and software could have been installed to monitor/spy on what you are doing. Even if the offender no longer has access to the physical device does not mean they're not accessing remotely. Here are some things to check on the Mac device:

Accessing remotely

Remote login - Computers that run macOS as an operating system can log in to your Mac using Secure Shell (SSH).

- Steps to check remote login - Apple menu > System settings > General > Sharing > Remote login > if remote login is checked, uncheck it.
- If there are any users you do not recognise on the list, you can remove them by list > select the user > then click the Remove button.

Remote desktop with remote management - it is possible to login to a computer with macOS by enabling Remote Desktop with management.

- Steps to check remote management - Apple menu > System settings > General > Sharing > Remote management > if remote management is checked, uncheck it.
- If there are any users you do not recognise on the list, you can remove them by list > select the user > then click the Remove button.

Screensharing - there is also screensharing which will allow someone to view someone's screen in real-time.

- Steps to check screensharing - Apple menu > System settings > General > Sharing > Screensharing > if screensharing is checked, uncheck it.
- If there are any users you do not recognise on the list, you can remove them by list > select the user > then click the Remove button.

Note - If a Mac is being monitored, it will show two rectangles in the top right-hand corner near the computer time.

With remote login and sharing options, an offender would need an account/user to sign into remotely. To find out all users on the Mac, a command can be used in the Mac terminal:

- **dscl . list /Users | grep -v '^_'**
  - If there are any accounts that are not recognised, then they could possibly have been created by the offender. To find out when all users have been used, type last into the terminal. This will list all the times and dates of logins. If there are times and dates for an account where there we logins at abnormal times, it is possible someone is accessing the Mac device remotely.

Keyloggers

Commercial keyloggers - offenders may have installed a key logger onto your Mac device to monitor what you are doing (some keyloggers can even take screenshots of the desktop). If you believe that the offender is monitoring you via your Mac, then there are possible ways to check for keyloggers.

- **Activity monitor** - this is the 'task manager' for Macs, it allows you to see what applications/tools are running currently on your laptop/computer. To open the activity monitor:
  - Applications > Utilities > Find and launch Activity Monitor.
- You can check to see if there are any unknown applications/tools that are running. Certain keyloggers will be named differently on activity monitor, check the name by searching it online, on a device you know is safe and secure.
- **Checking default key combinations** - Keyloggers have a key combination that will bring them out of hiding to the screen. Some common keyloggers:
  - Perfect keylogger: ctrl-alt-J
  - Elite Keylogger: ctrl-alt-S
  - Refog: option-shift-command-R
  - Spyrix: ctrl-alt-A
  - Revealer: ctrl-alt-F9
- Checking the list of application with Full Disk Access- most keyloggers must have full access to the disk or accessibility. To check this: System preferences > Security & privacy > Privacy > Accessibility and Full disk access.

Note - These are default key combinations, the offender may have changed them.

Malware keyloggers - MacOS has its own built-in antivirus technology called XProtect.

- If antivirus software has detected keylogging malware, find the malicious files/software, and remove them.

Malware

Malware is malicious software that can executed on a device and made to run code that can carry out activities on your device. Spyware (a type of malware) can not only be found on mobile devices, but on other devices too such as laptops/computers too.

Offenders can deploy spyware onto your Mac device to monitor what you are doing. Spyware can be installed by either physical access to the device or if a malicious email link is clicked on.

The built-in anti-malware protection on Mac OS X is known as XProtect. It scans applications and files for viruses and malware using a database that Apple updates daily. If it finds malware on a file or application, it immediately notifies the user and blocks the threat.

To check if XProtect is enabled:

Apple > System settings > General > Software Update > Advanced > Confirm there's a check next to 'Install system data files and security updates' or 'Install security responses and system files' (depending on your OS version).

Additionally, Mac Malware Removal Tool scans the entire system regularly to make sure nothing has slipped past XProtect. If it finds any malicious code, it immediately tries to defuse it.

Note - Although the security features of Mac are effective, you should not be discouraged from using third-party tools alongside XProtect.

Other guidance for Mac devices:

Make sure Wi-Fi is secure - a person's Wi-Fi router can be a weak link to their devices if they are not properly secured. Guidance on securing Wi-Fi routers can be found in above pages.

Check what has access to microphone and camera - check to see what apps can access your microphone and camera.

- System preferences > Security & Privacy - A list of apps will be shown.
  - Click on Camera and Microphone individually and check to see what apps are allowed access. If there are any apps that are not recognised, then they need to be removed.

Ensure that automatic updates are enabled - Mac devices should have automatic updates enabled by default, you should double check that your Mac device are downloading them.

- System preferences > software update > Advanced and ensure all the boxes are checked.

Make sure Mac's firewall is enabled - firewalls detect and protect your device from malicious traffic, and they should be always enabled. To check if your firewall is enabled:

- Mac settings > Network > Firewall

Using a privacy browser & VPN - MacOS comes with its own privacy browser, which allows you to visit and browse websites without them tracking your activity across multiple sessions. Private mode also ensures that webpages won't be stored in iCloud. This means that webpages you visit won't be shown from other devices connected to the iCloud. To always browse privately:

- Safari > Preferences > click General > click 'Safari opens with' then choose 'a new private browser'.

You should also ensure that you are using a VPN on their Mac devices. Be careful what you click on and install - if you receive a text message, email, social media messages or any other type of message that looks suspicious, then you need to avoid clicking on any links. It's also encouraged to report suspicious messages to:

- Text message- forward them to 7726
- Email- report@phishing.gov.uk

Secure passwords - create a strong password to login to your Mac device, guidance on creating strong passwords can be found 27.

- Automatic login - ensure that auto login is disabled. This stops anyone gaining access to the device (if taken/stolen) and logging in straight away.
- Automatically lock the Mac device whenever its inactive - this prevents anyone being able to access the Mac device if it was forever reason left unattended.

Use a password manager (or iCloud Keychain) - Although it important to ensure the password to your Mac device is strong and secure, it's also imperative that your other accounts have secure passwords too. Because of this, it can often be difficult to remember all the passwords (which is why most people use the same passwords across all their accounts), iCloud keychain saves and securely stores account login credentials, passwords and payment card information using AES encryption. To set this up on MAC:

- Apple menu > System preferences > click on your name > click Cloud > Turn on Passwords & Keychain.

Note - There are external password managers that can be used across different operating systems (OS), this can be useful if you have a range of different OS devices.

Create passkeys - passkeys are a way of signing in to an app or website account, without needing to create and remember a password. A passkey uses Touch ID or Face ID to identify you.

Enable iCloud two-factor authentication - this provides an extra layer of security where you will be required to input a randomly generated one-time code along with your account password when attempting to log into your accounts. To set this up:

- System settings > Apple ID > Password & security > click on 'Two-Factor Authentication' > you will then be asked to enter your phone number that will receive the one-time password.

Create non-administrative accounts - as a safety precaution, you should create a standard user account to use when administrative privileges (manage & delete users, install & remove software and change settings) are not needed. If an offender was to gain access to your computer, the potential wrongdoing is limited. For example, if the offender wanted to install a spyware software, they wouldn't be able to without admin rights. To add a user or group on Mac devices:

- Apple menu > Settings > click 'Users & Groups' > 'Add user' below the list of users on the right (you may be asked to enter your password) > New user > choose the type of user and follow the instructions.

Windows devices

Microsoft Windows is a product line of operating systems developed and marketed by Microsoft.

An offender can access your laptop/ computer remotely or have planted malware to monitor you. They also may want to access your private files on your device, especially files that are linked to an ongoing case you have against them. Additionally, they could look for confidential files such as medical records, and even delete files.

Windows Devices - it can be possible that if the offender once had access to your laptop/computer, configurations and software could have been installed to monitor/spy on what you are doing. Even if the offender no longer has access to the physical device does not mean they're not accessing remotely. Here are some things to check on the Windows device:

Accessing Remotely

- If you believe or there are indications of remote access, the first thing to do is disconnect the device from the internet.

Note - For an offender to be able to set up the Microsoft Remote Desktop Connection (RDC) tool - your device must be running Windows 10 Pro or Enterprise / Windows 11 Pro or Enterprise.

Check what version you're running, if you're usure, you can find out by: Settings > System > About > Windows specifications.

If you have these specifications, then to check for RDC can be done by:

- Settings > System > Remote Desktop > if 'Enable Remote Desktop' is checked, uncheck it.
- If the RDC was enabled, then under 'User accounts' on the Remote Desktop page click on 'Select users that can remotely access this PC'. If there are any user accounts listed in the box that is unfamiliar to you or are unwanted, click on the user and then click 'Remove'.

Another thing to make sure of is that Windows Firewall is blocking the Remote Desktop Port, this is an extra safety measure that may have been disabled by the offender if they had set up RDC. To check the firewall is blocking RCD:

- Settings > search for 'Windows Defender Firewall' > on the left-hand side click 'Allow and app or feature through Windows Defender Firewall' > you will now see a list of all the apps that are allowed to communicate through the Windows Firewall. Once you have found the Remote Desktop rules (there should be three- Shadow (TCP), User Mode (TCP-in) and User Mode (UDP-in)), right click on each one > click disable.

It should also be noted that the offender could have installed an external remote desktop application. To check this, go to 'Task Manager' and check the list of currently running programmes and look for any that are suspicious or unfamiliar. Some popular remote access tools that may have been installed without your permission include: VNC, RealVNC, RemotePC, LogMeIn, GoToMyPC, ZoHo Assist and TeamViewer.

- If you find a remote desktop programme running, then you will need to uninstall them. This is done by:
  - Settings > Apps > Apps & features > find the app you want to remove > select 'More' > Uninstall.

Keyloggers

Commercial keyloggers - offenders may have installed a key logger onto your Windows device to monitor what you are doing (some keyloggers can even take screenshots of the desktop). If you believe that the offender is monitoring you via your Windows device, then there are possible ways to check for keyloggers:

- **Task manager** - this is the first quick way to check if there is a keylogger running in the background/backend of your Windows device. To check this, go to Task Manager > Processes > More details (found at the bottom of the tab) > here you will see all the apps and programs running.
  - You can check to see if there are any unknown applications/tools that are running. Certain keyloggers will be named differently on activity monitor, you can check the name by searching it online, on a device they know is safe and secure.

    If you see any strange/unknown programmes, right click on them > choose 'End Task'.
  - Also check 'Startup apps' on Task Manager (this will be found on the left-hand side of the tab)- this will show you all of the apps that will start running when the Windows device is logged in/on.

    Any apps that are known to be keyloggers or look suspicious, right click on them > choose 'Disable'.
- **Programmes and Features** - this will allow you to see all the programmes on your Windows device. This can be done by:
  - Control panel > programmes > programmes and features > this will let you see all the applications on your Windows device. Anything known to be a keylogger application or anything that looks suspicious or unknown, right click on it > Uninstall.
- **Check temporary files** - keyloggers can sometimes hide themselves in temporary files to avoid detection, this is because temporary files are often too cluttered to spot suspicious programmes. You can check these files by:
  - Settings > System > Storage > click on Temporary files (this will show all the contents) > check for the files that look suspicious and then press 'Remove files'.
- **Windows Defender** - this will detect keyloggers and any other malware. To ensure Virus and threat detection is enabled:
  - Windows settings > Update & Security > under Protection areas click on Virus & threat protection > Manage settings > turn on 'Real-time protection'.

Malware:

Malware is malicious software that can executed on a device and made to run code that can carry out activities on your device. Spyware (a type of malware) can not only be found on mobile devices, but on other devices too such as laptops/computers too.

Offenders can deploy spyware onto your Windows device to monitor what you are doing. Spyware can be installed by either physical access to the device or if a malicious email link is clicked on.

For Windows users, Microsoft Defender Antivirus is an effective tool that finds and removes malware from the Windows device. To scan and remove malware from a windows device:

Windows security > Virus & threat protection > scan options > select 'offline scan' > click 'Scan now'.

Note - Although Microsoft Defender is an effective tool, you should not be discouraged from using third party tools alongside Microsoft Defender.

Other guidance for Windows devices

Ensure Windows Defeder is set up properly - Microsoft defender is a built-in antivirus programme in every edition of Windows. This offers real-time protection against forms of malware (including spyware). How to ensure Windows Defender is enabled is explained above. Although Windows 10 and above automatically update and scan the device for malware regularly, you can perform different scans manually:

- **Full virus scan** - Windows security > Virus & threat protection > under 'current threats' click scan options > Full scan > click 'Scan now'.
- **Offline virus scan** - if you believe that you may have spyware on your device, then an offline scan can be used to detect and deal with tough malware. This is because some malware cannot be removed whilst Windows is running. To start an offline scan:
  - Windows Security > Virus & threat protection > under 'current threats' click scan options > Microsoft Defender Offline > click 'Scan now' > scan.
- **Microsoft defender firewall** - you should ensure that your firewall is continuously turned on, so check this:
  - Settings > update & security > Windows Security > Firewall & network protection > click turn on.
- **Reputation-based protection** - this is an extra safety precaution that you can take that evaluates the trustworthiness of software and applications. If it detects a file, software or application that's attempting to be downloaded with a low reputation score, the system alerts the user. It will provide the user options to block, quarantine or allow the file under certain conditions. To enable this:
  - Settings > Privacy & security > Windows security > App & browser control > turn on.

Do a permissions audit & access right - Window devices have permission settings to prevent applications from accessing certain data (includes contacts, location, camera, microphone etc). You should check your app permissions regularly to ensure no applications are overextending permissions it doesn't need. To check these permissions:

- Settings > Privacy (or privacy & security in Windows 11) > scroll down to the 'App permissions' section > go through permissions to check which apps are accessing data they don't need.

Use a privacy browser & VPN - when InPrivate tabs or windows are used, browsing data (e.g. history, temporary internet files and cookies) isn't saved on your Windows device once you're done. To open an InPrivate window:

- Microsoft Edge > Settings and More > click 'New InPrivate window'.

VPNs are an extra security measure that will improve online privacy and obfuscate the users IP address more about VPN's are covered on page 80.

Ensure Wi-Fi is secure - a Wi-Fi router can be a weak link to your devices if they are not properly secured. Guidance on securing Wi-Fi routers can be found in above pages.

Secure passwords - you should ensure that you create a strong password to login to your Windows device (guidance on creating strong passwords can be found (page of document)).

- Additionally, ensure that auto login is disabled. This stops anyone gaining access to the device (if taken/stolen) and logging in straight away.

Create non-admin accounts - as a safety precaution, you should create a standard user account to use when administrative privileges (manage & delete users, install & remove software and change settings) are not needed. If an offender was to gain access to your computer, the potential wrongdoing is limited. For example, if the offender wanted to install a spyware software, they wouldn't be able to without admin rights.

- Settings > Accounts > Family & other users > on the right-hand side click on 'Add someone else to this PC'.

Part Seven:

Guidance on Backing up your Data

A copy of your important data that's stored in a separate and secure location.

Guidance on backing up your data

A copy of your important data that's stored in a separate and secure location.

Any data that you back up by using the cloud can potentially be accessed by the offender if they know your login details. This can become a big risk if you have been gathering evidence of their behaviour and actions.

Backup data is stored via the internet (cloud storage) or on hardware devices (USB sticks, SD cards or hard drives). When you backup your data, it means that even if you lose access to the original data, it can be restored by the backup copy.

The reasons why we should backup our data:

- We get new devices and want to copy existing files onto them.
- When we lose a device, or it is stolen.
- A device is broken which had important data on it.
- Data on our devices gets deleted accidently.
- Our device is infected with a virus.

Although these are the reasons for which we all may backup our data, survivors of Cyberstalking and Harassment have additional motives. It is imperative that you keep evidential material that can be used against the preparator to assist with your case against them.

Because of this, it is vital that you backup your data, to ensure that even if the offender gets hold of the data on your devices or for the reason mentioned above, there will always be a safe and secure place the evidence is kept.

How to backup data

The National Cyber Security Centre (NCSC, 2024) gives guidance and tips on how people should backup their data:

Cloud storage

Most people use products from Apple, Google or Microsoft (Windows) which comes with the feature of cloud storage. With these accounts, a certain amount of cloud storage is given to the user for free and might be sufficient to save all important files (upgrading cloud to provide more storage is available if needed).

Apple iCloud - Files and folders that you store in iCloud Drive will stay up to date across all your devices.

- **Setting up iCloud on iPhone and iPad** - Settings > Tap on your name > Tap iCloud > under apps using iCloud, turn on iCloud Drive.
- **Setting up iCloud on your Mac** - Apple menu > System preferences > click on your name > click iCloud (if prompted sign in with Apple ID) > under apps using iCloud, click iCloud Drive > turn on 'Sync this Mac'.
  - To add the files from Mac Desktop and your Documents folder to iCloud Drive > turn on Desktop and Documents.
- **Setting up iCloud on your Windows device** - When iCloud is set up on your Apple device > download on your Windows device 'iCloud for Windows' from the Microsoft store > open iCloud for Windows > sign in with your Apple ID > to the right of iCloud drive, click the arrow button > Turn on iCloud Drive.

Google Drive - You can back up content, data, and settings from your phone to your Google Account.

- **Setting up Google drive on Android device**- Settings > Google > Backup (if this is the first time, turn on Backup by Google One and follow the instructions) > Tap Back up now.
  - Google One can take up to 24 hours, when data is saved 'On' will be below the data types you selected.
- **Setting up Google drive on Mac or Windows device** - Download Google Drive to either your Windows or Mac Device (you will find the links for the download on the Google Drive webpage) > on your device, open GoogleDriveSetup.exe (Windows) or GoogleDrive.dmg (Mac) > Follow the instructions to complete setup.

Microsoft OneDrive

- OneDrive cloud icon> OneDrive Help and settings icon > settings > click on Sync and back up > select 'Manage back up' > to start backing up files, toggle any folder that says 'Not backed up' > select 'Save changes'.

If you use a different cloud provider, refer to their website for instructions on how to back up data.

Note - Ensure that you protect your cloud accounts by using strong passwords and turning on two-factor authentication. This is to prevent unauthorised access to your backup.

Removable media - In cases where you're creating particularly large backups, then using removable media to back up files and folders is advised.

You can back up your data to:

- An external hard drive
- USB stick or thumb drive
- SD cards

Note - When removable media isn't in use, they should be disconnected from the device it is backing up data from. This is to prevent potential viruses on the device attaching themselves to the removable media too.

For cases where you're gathering and keeping evidence against the offender, having both cloud and removable media with the evidential material adds extra assurance against losing the data.

Part Eight:

Guidance for Smart Devices/Internet of Things

The Internet of Things is a network of connected devices and technology that enables communication between devices and the cloud.

Doorbell surveillance

Video doorbells let you remotely chat with visitors and keep an eye on deliveries from the screen of your smartphone. When these doorbells start recording, they immediately send you and alert.

An offender can use your doorbell surveillance to monitor you. They will be able to see when you leave and enter your home, and it can also be used to see who is visiting you. Additionally, the microphone feature can be used by the offender to speak to you.

Note - It should also be noted that for any other type of outdoor surveillance that you may have, check to see what devices are linked to the account and remove any devices that are unfamiliar or unwanted.

If you have doorbell surveillance such as a Ring doorbell for example, then you should check to see who has access to it.

This can be done by:

Ring doorbell:

- Tap the top menu > Control centre > Authorized client devices.
  - If there are devices on the account that look unfamiliar or unwanted, then you can delete one device at a time, or all devices at one (except the device which you are using).
- Ensure to change the password for the account and to also set up 2FA.
- In cases where the offender had set up the ring doorbell and have the admin account, then you should factory reset the device. This will mean that you can create your own separate account for the ring doorbell to link to.

Blink video doorbell:

- Settings > Account and Privacy > Manage mobile devices. You can remove unknown or unwanted devices by clicking on the trash bin icon and then confirming the action when promoted.
- Like Ring doorbell, you may have to factory reset the Blink video doorbell if the offender has the admin account.

Alexa devices/or devices with similar functionalities

Alexa and other devices can respond to simple queries and perform complex routines to provide information, entertainment, and general assistance to its users.

An offender can access your Alexa or Google Home Nest (and other similar devices) if they know the username and password to them. Offenders will use these devices to listen into conversations and can even be used to harass you. For example, they could use the microphone feature to speak to you and even switch lights on and off.

A lot of homeowners now have smart home devices such as Alexa and products similar. In a lot of cases around the UK, Amazon Alexa devices are increasingly being used by stalkers to terrorise people in their own homes (usually by ex-partners).

Note - Offenders may be listening in on conversations without you knowing, its advised that passwords should be changed to the accounts.

Alexa

The first step to take when securing your Alexa devices is by changing the password to your Amazon account, this is because Alexa is an amazon device that uses your account to link to it. Alexa has even integrated with smart door locks.

You will then have to change your Alexa password- Access the Alexa app on your device > Tap on the menu icon and select Settings > Account Settings > Change Alexa Password.

- 2FA should also be enabled. This adds another layer of protection when logging into an account.

If an offender once had access or you want to check what devices are linked to an Alexa device:

- Open Alexa app > Devices > Echo and Alexa > Echo device > Settings gear icon > Bluetooth devices > Forget devices next to the device you want to remove.

Note - If you are still conscious over the access an offender may have on your Alexa devices, then you can do a factory reset by pressing and holding the button for 20 seconds and waiting for the light ring to turn off and on again. The device will then enter setup mode.

Google Home Nest

Google home nest devices will have almost the same security measures as an Alexa, although how to carry out these measures may slightly differ.

- The email used for the Google nest should be secure (look at guidance for email addresses)
- Settings > account > manage account > account security > account password.
- 2FA should be enabled to ensure extra security.

You can check to see who has access to your Nest home by going onto the Nest app > settings > Family & Guests. Here you can see who has access to your Nest home, any unwanted or unrecognised devices can be removed.

- Google home app > Devices > Settings > Under the home name tap the profile icons of home members > select profile icon of member you want to remove > Remove.

Unlike Alexa, Google home nest has a voice match feature that learns your voice over time. This means that the owner of the device can stop third parties and unauthorized people from using Google homes voice functionality to access sensitive information.

- If you want to remove voice match, then you can do this through your Google home app. Settings > Google assistant > Voice match > uncheck a device to remove Voice match.

Smart TVs

An internet-connected television that offers a range of online features, such as on-demand content from apps and the ability to connect to other wireless devices like smartphones.

Smart TVs come with many functions that can be installed from an app store, and some can even have built in cameras and microphones. If you have a TV that comes with a camera and microphone, then offenders may misuse these features to monitor you.

Any accounts that are created or signed into on the smart TV should be safe and secure.

- You should ensure that the accounts being used have strong passwords that are not shared with anyone, and the email used cannot be accessed by anyone else.
- 2FA should be used where possible, especially when trying to make purchases. If someone tried to access accounts, then they wouldn't be able to without a passcode.
- If the TV is set up and has preinstalled apps, then you should ensure that the apps are secure by reviewing their settings. If you have a camera and microphone on your TV, some apps will ask to have permission to access them- you should disable these permissions where you can.
- Browsing settings should also be reviewed. Most browsers will offer 'Safe browsing' or something similar, which will prevent from devices connecting and sharing content to the web browser.
- Limit as much personal and financial information shared with the smart TV.
- Disable (cover up) the TV's camera and microphone - offenders can possibly gain access to these features remotely. You should restrict or disable your TV mic and camera via settings. If you are still worried about the camera, you can cover it using a webcam cover or tape.
- It is important to keep apps up to date (usually update automatically) and updating the systems firmware. This ensures that you aren't exposed to vulnerabilities found in the old software.
- Ensure that the Wi-Fi being used to connect the smart TV to the internet is secure.

If you are still conscious about the access an offender may have, then you can always perform a factory re-set. This will remove the TVs previous settings and accounts; you will be able to set up new accounts and access information. To perform a factory reset, you will have to go into the settings, each make may differ on where to find it.

Nanny cams/webcams

A video camera which is designed to record or stream to a computer or network.

Offenders can access nanny cams and webcams remotely; this allows them to spy on you by listening into conversations and watching what you are doing. With some webcams, you can even speak into them, the offender can speak to you via the nanny cam.

If you have nanny cams/webcams in your home, then there are a few steps you can take to secure them:

- Ensure that only recognised and authorised devices are linked to the webcam account- usually linked devices will be found in the settings section of the app and can be easily removed.
- Change the password for the nanny-cam/ webcam software/app. Ensure that a strong password is used (see advice on creating strong passwords)
- Ensure that the Wi-Fi network is secure (look at guidance given for Wi-Fi routers). This would be to stop the offender gaining access to the webcam by targeting the homes wireless router.
- Turn off the webcam when you are not using it and disconnect it from the internet. The nanny-cam/webcam should not be left on all day if it is not being used all day.
  - If you have webcam features on your computers/laptop or any other devices, then covering them when not being used is advised.
- Depending on what the nanny-cam/webcam is used for – you should keep in mind of the microphone. If the microphone is not needed, then it should be disabled to prevent an offender from listening into conversations.

Home hub systems

Smart home hubs are used to control and power a range of smart home devices from one location (the hub).

An offender can access your Home Hub (and other similar devices) if they know the username and password to it. Offenders can use the Home Hub to harass you. For example, they could use the hubs feature to turn lights on and off in your home and can control other connected devices on the Hub.

Home hubs have become a popular technology that are used in people's homes. These hubs can be accessed remotely, which means that anybody who has access to your hub can monitor what you are doing in your home or even make changes.

If you have one of these hubs in your home, then there are a few safety tips you can take to ensure its secure:

- **Ensure the ADMIN password has been changed** - even if you have changed passwords for user accounts on the hub, if the offender has the admin password, they will continue to have access to the hub. Guidance on how to change the admin password can be found on the website of the Hub you have (e.g. Google, Echo Hubs).

Note - In some cases where the offender set up the Hub, factory resetting the hub may have to be an option.

- **Check if the Hub is automatically storing your data** - this data could be your location history. If the offender was to gain access to your account, they could access this information and find out where you have been or where you have been going. You should go into your Hub settings and consider disabling this feature.
- **Voice activation** - if you don't use the voice activation feature, you should consider muting/disabling it on their Hub. This is because if the offender has access to the Hub, they could remotely activate the microphone and listen in on conversations. You should go to your hub settings and consider disabling this feature.
- **Linked accounts** - You should review what accounts are linked to your Hub. Accounts that hold personal/sensitive information about you (banking, medical data etc) should not be connected to the Hub. For example, if the survivor uses Google or Echo, you should use a separate Google or Amazon account specifically for the Hub and home devices.
- **Turn off the hub whilst you are away** - if you're away, the Hubs don't have an off/on button (usually). You should unplug the devices connected to the hub you won't need whilst you're gone.
- You should turn off your internet connection to your hub when it is not in use.
- **Ensure the Wi-Fi is strong and secure** - guidance is given on Wi-Fi routers which can be found in above pages of this document.
- **Software updates** - Ensure that you keep up to date with software updates, this ensures security features of the device are up to date and more difficult to override.

Devices gifted by the offender

An offender could have bought or installed listening devices and cameras. These can be put into many different objects and given to you as a 'gift' or discretely planted somewhere in your home.

If you were once in a relationship with the offender or any sort of relationship that was offline, then you should try to remember any gifts that were given to you by the offender. This should even include possible items that they had 'accidently' left behind in the house, or items that were given to the children (if applicable).

Hidden cameras, listening devices and trackers can be hidden in pretty much anything. If the offender knows details of conversations you're having in your home, or knows what you are doing in your home, then it could be possible that a hidden camera or listening device has been planted.

Note - It's important that if applicable, extensive searches in the home are undertaken.

Part Nine:

Guidance in Car Tracking

Monitoring the location of a car or any moving vehicle using the GPS system.

Physical car trackers

An offender can plant physical trackers in or outside of your car as a method to monitor and follow your location.

Locating through planting trackers

In some cases, an offender will go to the lengths of planting a small tracking system on/in your vehicle.

- Real time vehicle tracking devises (attached) can be bought on Amazon for as little as £20, this makes them very accessible for offenders. Some of these trackers can be found attached to the battery of the vehicle, some trackers are even magnetic which can be planted inside or out of the vehicle.
- Real time tracking devises (unattached) can be used in vehicles and can be hidden anywhere. These tracking devices are usually small in size, which means that they may be hard to spot/find if they were hidden in a vehicle.

If you or officers have a reason to believe that your vehicle is being tracked, then the right searching methods should be taken (speak to officers about the right steps to take regarding this). Additionally, there are GPS blockers and signal jammers that can be bought online (for extra precaution). These are designed to disrupt signals received by GPS trackers and prevent them from functioning.

Dashcams

A dash cam is a small video camera. It is attached to the car's dashboard or windscreen in a position that gives a good view of the road ahead. It records footage as you drive along.

An offender can access your dashcam footage to monitor and locate where you have been going. It can also be used to monitor your location in real-time.

If you have a dashcam then you should check to see who has access to the footage. An offender can access and view this footage to see where you have been travelling or where you are.

- Most dashcams come with dedicated apps with built in Wi-Fi that allow a person to connect and sync up from their phone or tablet and view the footage from there.
- Your dashcam might have a dedicated app, if you use the app, you should change the password and ensure that no one else has access to the account.
- Some dashcams may offer encryption features to protect footage from being accessed by unauthorized individuals- you should check on the dashcams website to see if this feature comes with your dashcam. If so, it would be a good idea for you to enable this feature.
- In cases where the dashcam was set up by the offender, they may have been the one to have access to the dedicated app. If you do not know the account details of the app, you should factory reset the dashcam. Guidance on how to factory reset the dashcam will be found on the dashcams website. By factory resetting the dashcam, it should disconnect from the account on the app.

Part Ten:

Guidance for Third Parties

An offender can bait/trick third parties into disclosing information about you to them. Additionally, anything that third parties post about you online may be seen by the offender.

Often, offenders will use family and friends to get to you. This sort of tactic can be made easier if:

- **You and the offender have mutual friends** - mutual friends could be relaying back information to the offender about you unknowingly.
  - **Baiting for information about the survivor** - if the mutual friend speaks to both the offender and you regularly, then there comes the risk of sharing information. For example, the offender could ask the mutual friend on how you're doing (coming across concerned), or the mutual friend could mention upcoming plans they have with you. The offender could bait the mutual friend into disclosing the location of these plans.
  - **Social media** - if the mutual friend has both you and the offender on social media, they should not be tagging you in photos or disclosing the location.

Because of this, it is important that third parties are made aware of the offender's behaviour/ actions, and they should ensure not to speak about you with them. Additionally, mutual friends should not tag you in photos on social media or disclose personal information (such as location) about you.

- You both share children with one another - it can be hard to cut all strings with the offender when children are involved (depending on the circumstances) so contact with you or family members relating to the children may apply.
  - **Baiting family members for information** - like mutual friends (which is mentioned above) the offender may bait family members into disclosing information you. Family members should try their best to avoid conversation relating to you and keep it strictly to about your children.
  - **Social media** - family members should also be careful on what they post online, and to limit photos or information they post about you. If they are to post photos of you, ensure that their account is not tagged, or the location is not disclosed.

In the best-case scenario, third parties should block the offender from their social media accounts and should be made aware of any impersonation accounts that the offender may have created of you.

Third parties should not disclose any personal information about you to the offender (mutual friends or family), this includes where you live, work, your social plans, mobile number etc.

Offenders will do anything to gain information about you, so third parties should be careful about what they disclose online or in person.

Part Eleven:

Computer Misuse Act (CMA) 1990 and Sexual Offences Act (SOA) 2003

Computer Misuse Act (CMA) 1990

This is a key piece of legislation in the UK that makes unauthorised access to, and modification of, computer data illegal.

Offences that are covered by the sections of the Computer Misuse Act (1990) will without doubt be relevant in a survivor's case relating to online stalking and harassment.

Section 1 of the Computer Misuse Act

This section deals with the offence of unauthorised access to computer material.

For example - the offender knew or guessed the survivor's password and accessed their social media account/s without permission.

Note - If the offender has accessed any of the survivors' online accounts, or devices without consent, then they are committing a CMA offence.

Section 2 of the Computer Misuse Act

This section deals with the offence of unauthorised access with intent to commit or facilitate a further offence.

For example - the offender accesses the survivors online banking app without consent with the intention of stealing money.

Section 3 of the Computer Misuse Act

This section deals with the offence of unauthorised acts with intent to impair the operation of a computer.

For example - the offender accesses the survivors Wi-fi router without consent, changes the password and knocks their devices off the internet.

Section 3ZA of the Computer Misuse Act

This section deals with the offence of unauthorised acts causing or creating the risk of serious damage.

Note - This CMA offence will not apply to cases of online stalking and harassment and is aimed at those who seek to attack critical national infrastructure.

Section 3A of the Computer Misuse Act

This section deals with making, supplying, or obtaining articles (a program or data held in electronic form) for use in sections 1, 2 and 3.

For example - If an offender obtains Malware with the purpose of deploying it on a survivor's device- but has not yet or had the chance to deploy it.

It is important that officers and you are aware and understand the elements of these offences. By doing so, you and officers will be able to identify these offences when they are taking place. This will allow for preservation of evidence for any potential future action against the offender.

Sexual Offences Act (SOA) 2003 as part of the Online Safety Act (OSA) 2023

You should be made aware that it is now a criminal offence to share intimate images or film without consent, regardless of whether the offender intended to cause the survivor any harm.

The Sexual Offences Act (2001), s 66(b) brings in three offences of sharing intimate images:

1. A person intentionally shares a photograph or film that shows, or appears to show, someone in an intimate state without their consent.
2. A person intentionally shares a photograph or film that shows, or appears to show, someone in an intimate state with the intention of causing alarm, distress, or humiliation to that person and without their consent.
3. A person intentionally shares a photograph or film that shows, or appears to show, someone in an intimate state with the purpose of their own or someone else's sexual gratification, without the consent of the person in the photograph or film, and without the reasonable belief that they consent.

It also brings in a fourth offence of threatening to share intimate images.

4. A person threatens to share a photograph or film that shows, or appears to show, someone in an intimate state. They either intend that the person in that intimate state, or someone who knows them, will fear the threat being carried out, or they are reckless about that person's fear of it being carried out.

StopNCII.org

StopNCII.org is a free tool designed to support survivors of Non-Consensual Intimate Image (NCII) abuse. The tool works by generating a hash from your intimate image(s)/videos(s). StopNCII.org sends the hash with participating companies so they can help detect and remove the images/videos from being shared online.

Participating companies:

facebook, TikTok, reddit, Instagram, bumble, OnlyFans, Threads, Pornhub, Snap Inc., NIANTIC, playhouse, REDGIFS

To find out more about this project operated by the Revenge Porn Helpline, visit their website at www.stopncii.org.

Additionally, Google have support resources for removing explicit or intimate personal images on their search engine.

StopNCII.org

Request removal of content on Google Search

Part Twelve:

Artificial Intelligence (AI)

Allows computers to learn and solve problems like a person. Computers are trained on vast amounts of information and learn to identify the patterns in it, to carry out tasks such as having human-like conversation.

Artificial intelligence (AI) is the forefront of evolving technology, its potential to increase efficiency and make information widely available is almost limitless. However, due to its prevalence, we must recognise and consider its impact on facilitating Violence Against Women and Girls:

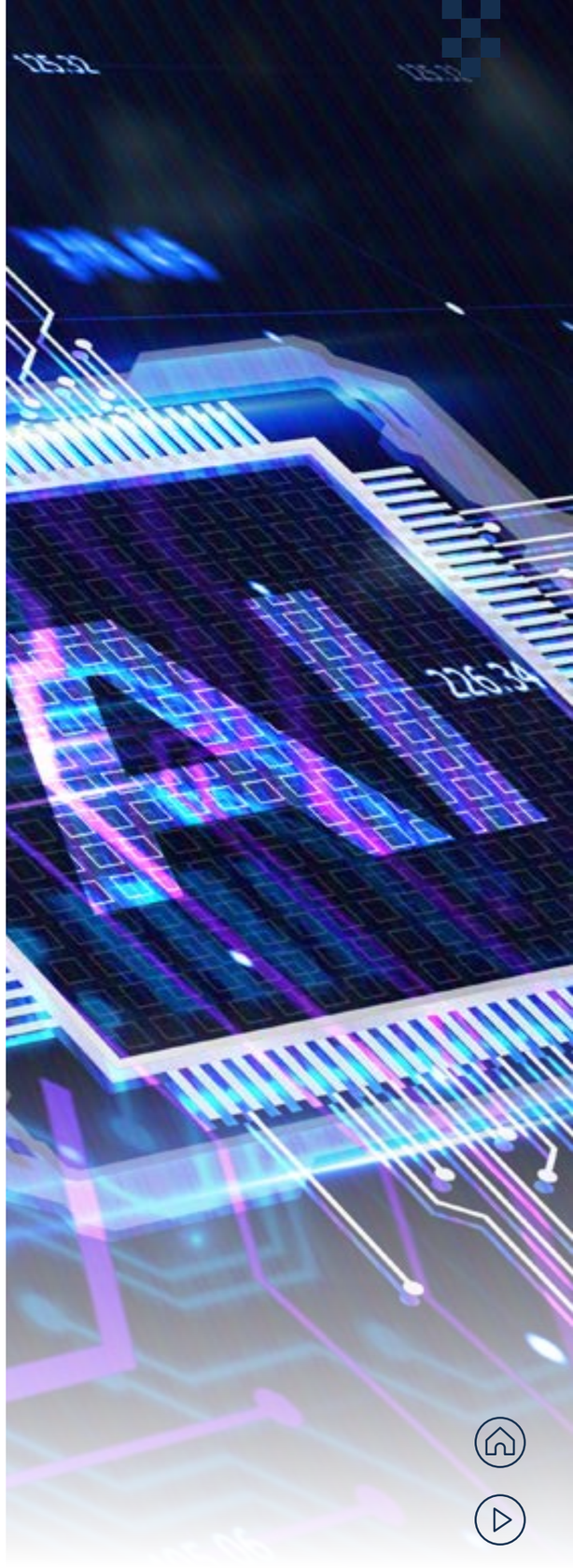
What may be happening

AI & Stalking - the offender could be using AI to monitor and track you with better accuracy and at more ease. For example, AI powered algorithms could analyse and predict your location by gathering data from sources such as social media and geotagged images.

What we know is happening

Deepfakes (deep learning + fake) - uses deep learning algorithms to create convincing fake images and videos. This technology has and continues to be used against women to create and mimic nonconsensual pornography. The offender no longer needs to receive an intimate image but instead just create one using AI.

Note - Under the Online Safety Act, the sharing and creation of deepfakes is an offence.



References

College of Policing (2024) Violence Against Women and Girls (VAWG)- National Policing Statement 2024. [Accessed 23 July 2024]

Computer Misuse Act (1990). [Accessed 24 July 2024]

Crown Prosecution Service (2019). Violence against Women and Girls Guidance. [Accessed 2 August 2024]

National Cyber Security Centre (2024). Top tips for staying secure online [internet]. [Accessed 8 July 2024]

Office for National Statistics (2023). Experiences of harassment prevalence and nature tables, England and Wales [internet]. [Accessed 26 June 2024]

Online Safety Act (2023). [Accessed 24 July 2024]

Refuge Tech Safety (2024) Digital Breakup. [Accessed 26 June 2024]

South Wales Police (2024). Tackling Violence Against Women and Girls - National Policing Statement 2024. [Accessed 24 July 2024]

STRA forthcoming end of 2024 - Bespoke data collection across all forces of police recorded crime in 2023/24 to inform an assessment on the threat of Violence Against Women and Girls.

STRA forthcoming end of 2024 - Bespoke data collection exercise conducted by the CSAE analysts' network for the STRA.

STRAVA (2024) Activity Privacy Considerations. [Accessed 8 June 2024]

HEDDLU
DE CYMRU
SOUTH WALES
POLICE

Mae'r ddogfen hon hefyd ar gael yn Gymraeg.

This document is also available in Welsh.