National Cyber Security Centre
a part of GCHQ

Last updated: 3rd February 2026

Technology-facilitated domestic abuse, stalking and cyber crime guidance

Advice for domestic violence practitioners to help victims who are being tracked, stalked, or virtually monitored using digital technology

Contents

Introduction **4**

Securing victims' devices **5**

Changing passwords/passcodes (or fingerprint/face ID) 5

Turning off location tracking 5

Turning off location tracking on your device **5**

Turning off location tracking on individual apps **6**

Use iOS Safety Check for iPhones 6

Fitness trackers and smart watches 6

Emergency contacts/SOS messages 6

Additional device safeguarding guidance 7

Removing tracking software **9**

How to tell if a device has been hacked 9

Resetting devices 10

Protecting phone calls **11**

Using video conferencing safely **12**

Protecting online accounts and files **13**

Protecting photos and videos that are stored in the cloud (online) 13

Deleting internet history 13

Recovering social media accounts 14

Bank accounts/online banking 15

Securing home wi-fi **16**

Changing your internet router settings 16

Securing smart devices and IoT risks 17

Key Risks and Actions **17**

General Advice **17**

Deleting the search history from smart devices 18

Gas and electricity 'smart meters' 18

Vehicle tracking **19**

Bluetooth Trackers (Air Tags, Tile, etc.) **20**

Preventative measures **21**

Creating strong passwords 21

Take special care of email passwords 21

Keep your devices updated....22
Antivirus and Malware Protection....22
Add extra security by setting up 2SV....22
Make sure stolen devices can be tracked, locked and wiped....22
App Protection and Privacy Settings....23
Using Public Wi-Fi Safely....24
VPN Use and Limitations....24

Introduction

This guidance has been produced to support practitioners working with victims of technology-facilitated domestic abuse cyber crime. Practitioners can use this advice to help victims who are being tracked, stalked, or virtually monitored using digital technology. It includes a section on preventative measures that victims can take to reduce the likelihood of an abuser being able to monitor their devices and accounts.

The National Cyber Security Centre (NCSC) will continue to update this guidance in line with feedback from charities, law enforcement, and independent domestic violence advisors (IDVAs). Please send any feedback to feedback@ncsc.gov.uk.

Due to the exceptional circumstances that victims of domestic abuse find themselves in, this document may deviate from 'standard' NCSC guidance. Where this is the case, we'll explicitly point it out.

Note: **While this guidance contains up-to-date technical advice, it does not make any attempt to assess the risk of applying this advice. Practitioners should consider the individual circumstances of each person they are working with, in particular whether implementing this advice could put the victim in greater danger.**

For example, if a victim changes their password, the abuser will probably realise what has happened when they attempt to log in, and this could lead to an escalation of abusive behaviours. It is up to the IDVA, or suitably qualified professional, to decide how the purely technical advice presented here should be adopted, in order to prioritise the safety of the victim.

Securing victims' devices

There are a few things a victim can do to make it more difficult for an abuser to track them, whether the abuser is:

- accessing a phone (or tablet, or laptop) directly
- monitoring the victim's location via social media activity
- using tracking software

If the abuser has physical access to the device, the victim can prevent them from being able to use it by setting up a password (or passcode), a fingerprint lock or face ID lock. This effectively 'locks' the phone when it's not in use, so only the owner (or someone who knows the password) can access it.

For detailed instructions on how to do this, please refer to the following links.

- How to set a passcode on an iPhone/iPad device (Apple phones and tablets).
- How to set a passcode on an Android device (such as those manufactured by Google, Huawei and Samsung).
- How to set a passcode on a Windows computer.

Changing passwords/passcodes (or fingerprint/face ID)

If the victim suspects the abuser already has access to the device, they may want to change it so that the abuser can't unlock the device. Or they can set up Touch ID (fingerprint recognition) or Face ID (face recognition).

- How to set up Touch ID on an iPhone/iPad device.
- How to set up Face ID on an iPhone/iPad device.
- How to change the screen lock on an Android device (such as those manufactured by Google, Huawei and Samsung).

Turning off location tracking

Many social media apps use location tracking to show friends and followers where they are, or where they've posted a message from. An abuser can also see these updates. If the victim thinks these apps are being used to track them, they can turn off location tracking for individual apps. Alternatively, they can disable the location services on the device, so that *none* of the apps (or followers) can access the location of updates posted from that device.

Turning off location tracking on your device

Turning off location tracing on the device will prevent some apps from working, such as mapping software. Victims will also be unable to use tools to lock/find/erase the data on phones that have been lost or stolen.

- Turn off location tracking on an iPhone/iPad device (Apple phones and tablets)
- Turn off location tracking on an Android device (such as those manufactured by Google, Huawei and Samsung)

Turning off location tracking on individual apps

- Turn off location tracking in Facebook
- Turn off location tracking in Find My Friend
- Turn off location tracking in Instagram
- Turn off location tracking in Snapchat
- Turn off location tracking in X

For more information about how to manage the security and privacy settings on social media accounts, refer to the NCSC guidance on using social media safely.

Use iOS Safety Check for iPhones

Why use it?
iOS Safety Check is an emergency privacy feature on iPhones (iOS 16+) that allows users to quickly stop sharing information and secure their device. It provides an all-in-one option to revoke location sharing, reset app permissions, and review account security in urgent situations.

Fitness trackers and smart watches

When using smartwatches or fitness trackers (such as Fitbit, Apple Watch, and Garmin Smart Watch), ensure that routes and activities are not being shared publicly, as these can provide information about where victims have been. For more information about keeping routes private, refer to the following resources.

- Strava: Training Log Privacy Controls
- Garmin: Adjusting Privacy Settings in Garmin Connect
- Fitbit: FAQs on Privacy: Fitbit - Help
- Apple Watch: Manage Activity sharing on Apple Watch - Apple Support (UK)

Emergency contacts/SOS messages

Many phones and smart watches/fitness devices can be configured to send your last known location to emergency contacts.

Note: Whilst this function is invaluable for many users who find themselves in an emergency, if a named emergency contact is an abuser, the victim may want to update (or remove) this information.

Refer to the following resources for information about how to do this:

- Apple: Use Emergency SOS on your iPhone
- Android: Get help in an emergency using your Android phone

Additional device safeguarding guidance

In addition to setting strong passcodes and enabling biometric locks, practitioners should consider the following measures to protect victims from physical and digital compromise:

Biometric Risks

While fingerprint and face recognition can be convenient, they pose specific risks in domestic abuse situations. For example:

- An abuser could use a victim's fingerprint while they are asleep or unconscious.
- Face recognition may work even if the victim's eyes are closed unless "Require Attention" (iOS) or "Require Open Eyes" (Android) is enabled.

If these options are unavailable or unreliable, advise victims to use a PIN or password instead. Testing these settings is recommended.

App-Level Security

Many apps (e.g., banking) allow biometric login. Victims should avoid using biometrics for apps and instead use strong PINs or passwords. This prevents an abuser who unlocks the device from accessing sensitive apps without additional credentials.

Private File Storage

Victims may need to store sensitive evidence (photos, notes). Options include:

- Secure folders (e.g., Samsung Knox) with separate PINs or passwords.
- Hidden or locked content features on Apple iOS and Android.
- Trusted third-party apps designed for secure storage.

Note: No method is completely undetectable if the abuser has extensive access. Consider sending files to a trusted person and deleting originals.

Masquerading Apps

Some apps disguise themselves (e.g. Bright Sky appears as a weather app). While useful, these should be used cautiously, as an abuser can easily identify them by name.

SIM PIN Protection

Setting a SIM PIN prevents an abuser from moving the SIM to another device to intercept calls or 2SV codes. However:

- It is not common practice and may alert the abuser.
- Incorrect attempts can lock the SIM, requiring provider intervention.

Most phones have a default SIM PIN set but not activated. Before setting your own SIM PIN you should find out the default PIN for your provider.

Emergency Alerts

Government emergency alerts can reveal a hidden phone. Victims can opt out via device settings:

- iPhone: Search "Emergency Alerts" and disable Severe/Emergency alerts.
- Android: Search "Emergency Alerts" and disable Severe/Emergency alerts.

See UK Government Emergency Alerts guidance for details.

Useful Resources

- Apple Safety Check – Stop sharing and review security
- Samsung Knox Secure Folder – How to set up and hide
- Hide Photos on iOS – Apple Support
- Lock Notes on iOS – Apple Support
- Google Safe Folder – Protect your files

Removing tracking software

If abusers don't have physical access to the phone, the most common way to monitor victims is to trick the victim into installing spyware. This is usually done by sending a scam email, social media post, or text message (the NCSC has guidance to help spot these scam messages).

Spyware can also be bought online legally, and doesn't require much technical knowledge to operate. Examples include Flexispy and Web Watcher. These applications are often advertised as 'parental control' or 'employee monitoring' software and may have legitimate uses, but they can also be used for malicious purposes to track people.

Victims can remove any apps from devices that they've not installed themselves, including tracking/stalkerware.

- Delete apps from an iPhone/iPad device (Apple phones and tablets)
- Delete apps from an Android device (such as those manufactured by Google, Huawei and Samsung)
- Uninstall apps and programs from Windows
- Uninstall apps on your Mac

Note: If victims remove applications (or reset the device), the abuser responsible for adding the stalkerware will likely be alerted.

How to tell if a device has been hacked

It can sometimes be difficult to know if a device has been hacked. However, some things to look out for include:

- the device is running slowly
- the device keeps rebooting
- the device's battery runs out quickly
- excessive data use
- the device gets very warm
- apps start automatically
- emails that report logins from unusual locations
- emails that report logins from devices that you don't recognise
- unexpected messages from apps
- someone receives messages that the victim has not sent

If a victim believes they have been hacked, they should make a note of any irregular messages or behaviour (if it is safe to do so).

Resetting devices

There is no need to dispose of a device if the victim believes there is spyware on it. Instead, victims can start by trying to remove any apps that they don't recognise, as described above. Some spyware is designed to be installed stealthily, so the victim cannot see it. In such cases, victims can perform a factory reset, which will delete all apps (including stalkerware) that have been manually installed. For information about how to do this, please refer to the NCSC's guidance on resetting your device. This includes how to make sure you don't lose important information, such as photos, documents and passwords.

When resetting a device especially a second-hand device or one previously controlled by an abuser always use the official factory reset process for your platform. This ensures all unwanted apps and data are removed.

Factory Reset Instructions:

- Reset your Android device to factory settings
- How to factory reset your iPhone, iPad or iPod touch
- Reset your Chromebook to factory settings
- Reset your PC
- What to do before you sell, give away, trade in or recycle your Mac

Migrating to a New Device Safely

When moving from an old device to a new one:

1. Reset the new device first to remove any pre-installed apps or malware.
2. Back up and transfer data carefully:
    - Avoid transferring apps directly if you suspect spyware; reinstall apps from the official app store.
    - For cross-platform migration:
        - Switch to a phone that feels like you.
        - Move from Android to iPhone or iPad
3. Ensure account access before erasing old device:
    - Confirm you have login details and 2SV set up for email, social media, and banking.
    - If using SMS or authentication apps for 2SV, verify these work on another device before wiping the old one.
4. Set up the new device securely:
    - Enable device lock (PIN/password).
    - Configure app-level security.
    - For laptops/PCs, activate built-in antivirus and firewalls.

Protecting phone calls

It's unlikely that abusers have the resources to tap their victim's landlines in order to listen into calls. If you believe this is the case, the police can be contacted on 101, and asked to investigate. If victims believe their phone has been tapped, they should use an alternative means (such as mobile phone, or a trusted family or friends' phone).

However, it is simple for an abuser to access a victim's voicemail (from another number) unless voicemail is protected with a PIN. Here are instructions for how to do this:

- Vodaphone: How do I set up a security PIN on voicemail
- EE: How do I set up security on my voicemail
- O2: Protecting your voicemail
- Three: Keeping your voicemail secure

For instructions for other network providers, refer to the support area on their websites.

Preventing Call Interception and Stalkerware Risks

- Common stalkerware apps can record conversations on mobile devices. If victims suspect this, they should follow the guidance in the "Resetting Devices" section to perform a factory reset and reinstall apps manually from official app stores.
- For sensitive calls, victims may wish to use another trusted mobile phone or landline that the abuser cannot access (e.g., a friend's phone or workplace landline).
- Landline tapping is rare, but if suspected, victims should contact the police on 101.

Using video conferencing safely

The increased use of video conferencing technology in recent years mean many of us are now using video calls to stay in touch with family, friends and work colleagues. Even if victims are familiar with video conferencing, they should take a moment to check how they're using it. For more details, you can refer to the NCSC's guide to using video conferencing services.

Many devices have video conferencing functionality built in (such as Apple's FaceTime and Google Meet), and many popular apps also provide this service (such as Instagram, WhatsApp and Facebook). There are also standalone video conferencing apps that you can download; popular titles include Zoom and Microsoft Teams.

Whatever application is used, victims should be able to control who can join a video conferencing call that they are hosting. For specific instructions, refer to the support website of the service being used. However, the following general rules apply:

Do not make the calls public. Victims should connect directly to participants using their contacts/address book, or provide private links to the individual contacts. For some video conferencing services, victims can set up the call so that a password is required to join. Victims should not post the link (or the password) publicly.

Know who is joining the call. If victims are organising a call for multiple guests, they should use the 'lobby' feature to ensure they know who has arrived. This is especially useful if individuals are joining the call via an unrecognised phone number.

Understand what can be recorded. Some video conferencing tools will notify users if the meeting is being recorded, or if a screenshot has been taken. However, it is impossible to prevent a screenshot or image being taken during a video call.

Consider the surroundings. Victims should take a moment to think about what their camera shows when on a call. Most popular video conferencing tools allow the background to be blurred or changed completely, so the location can't be easily determined.

- Zoom: Using a blurred background
- Microsoft Teams: Change your background for a Team meeting
- Google Meet: Change background and use effects in Google Meet

They may also want to consider making video calls away from home or a sensitive location, such as from a refuge.

If victims are using a laptop with a built-in webcam, one solution (when it's not in use) is to stick a piece of dark tape over the lens, so even if someone does have access to the webcam, they will not be able to see anything from it. They can also choose to turn off the webcam and the microphone in the device settings. If it's an external (ie USB) webcam, it can simply be unplugged when not in use.

If an abuser is technically adept, they could determine the approximate location of a victim on a video conference by working out their IP address. If you suspect this is a possibility, victims can make video calls using the phone's mobile network, rather than using their wi-fi connection, as this will make it much harder to identify the IP address. However, video conferencing is bandwidth intensive, so making calls this way may incur excessive data charges.

Protecting online accounts and files

Family or group sharing is a feature that allows family members to share media such as photos or calendars, but also locations and diaries. Victims should check their account settings to see who they are sharing their location (and other resources) with. They can change these settings within the account, or turn it off completely.

- Leave Family Sharing – Apple Support (UK)
- Start or stop sharing with your family - Android - Google One Help

Victims can control who is able to access the 'shared albums' feature by following this guidance from Apple.

Protecting photos and videos that are stored in the cloud (online)

Data stored on devices (such as photos, videos and documents) is often automatically backed-up online, so that you have a copy of files that you can restore in case you lose or damage your device. Victims should use a strong password to control who has access to this information, and also turn on two step verification (2SV), which will provide an extra layer of protection. This will limit the opportunities the abuser has to access any explicit images, and post these online without consent (commonly known as 'revenge porn').

If victims' images have been shared online without consent, they can contact the Revenge Porn Helpline, who can help and support victims of intimate image abuse. Sharing (and threatening to share) sexual content is a criminal offence under the new 2021 Domestic Abuse Act.

Deleting internet history

The majority of internet browsers (Google Chrome, Apple Safari, Microsoft Edge, Mozilla Firefox) offer a 'private' search option when browsing the web. When turned on, this ensures that neither the browsing history (that is, a list of websites visited) nor any passwords are saved.

- Use Firefox without saving history
- Using Private Browsing in Safari on Mac
- Google Chrome: Browse in private
- Browse InPrivate in Microsoft Edge

However, using the private search option **doesn't** delete the history of websites previously visited. To delete the full history, refer to the following resources:

- Clear cookies and site data in Firefox
- Remove website data in Safari on Mac
- Clear browsing data from Google Chrome
- View and delete browsing history from Microsoft Edge

Additionally, if victims have an associated online account (either a Gmail account or Microsoft account), they can delete their search history by logging into it. They can also disable this feature so the browser search history will not sync with their associated online account.

- Check or delete your Chrome browsing history

- View and manage your Yahoo! search history Yahoo Help
- Manage your Microsoft account search history

Recovering social media accounts

If the victim has lost access or control of a social media account, the social media provider can help. Once the victim has confirmed their identity, the passwords can be updated. If the abuser is impersonating a victim on a social media account, they can request that the fake account is shut down. Refer to the links below for more information.

Note some platforms (such as Facebook or Instagram) allow you to sign out from another device. Victims may need to do this (and then change their passwords) so abusers can't log back into the account. Many social media sites have a feature that enables users to view the devices they are logged into, and to sign out of any they don't recognise.

Guidance from a range of social media providers can be found in the following links:

- Facebook: report a compromised account
- X: Account is hacked or compromised
- I think my Instagram account has been hacked
- Snapchat: my account is hacked, my account is compromised - Snapchat Support
- LinkedIn: Reporting a compromised account
- Reddit: I need help with a hacked or compromised account
- Tinder: Security FAQs - I think my account has been hacked
- Tik Tok: My account has been hacked

For more information about how to manage the security and privacy settings on social media accounts, refer to the NCSC guidance on using social media safely.

Bank accounts/online banking

Victims should address any concerns around banking (including online banking) directly with their bank, as each bank will have specific measures (such as flagging up fraud warnings) to help the victims, especially if the perpetrator has access to a joint account. However, all banks will give you the option to Set up 2-Step Verification (2SV). You should always set this up, as it adds extra security to your online banking.

Victims should address any concerns around banking (including online banking) directly with their bank, as each bank will have specific measures (such as flagging fraud warnings) to help protect them especially if the perpetrator has access to a joint account.

If possible, open a separate account in your name. Online only banks (such as Monzo or Starling) may be easier to set up. Change any PINs or passwords you think the abuser knows.

Enable 2-Step Verification (2SV). for online banking. You should always set this up, as it adds extra security even if the abuser knows your password. Banking apps may not use 2SV for login but may require it for certain transactions. Avoid using biometric login (fingerprint or face ID) if you live with the abuser.

Other steps:

- Switch to paperless statements so there is no physical copy for an abuser to access.
- Be aware that using cash avoids a digital trail, but withdrawing cash may raise suspicions.

If you believe the abuser may try to open accounts in your name, consider CIFAS Protective Registration. This adds a warning flag to your details in the National Fraud Database and helps prevent identity fraud. More information: https://www.cifas.org.uk

Securing home wi-fi

The range of a typical domestic Wi-Fi network will usually extend beyond the boundaries of the victim's property. This means that if an abuser knows the Wi-Fi password (or can access the victim's router), they could access a Wi-Fi network from the road outside a home. Furthermore, they can use widely available software to analyse what websites the Wi-Fi is accessing.

If the abuser has previously had access to the victim's Wi-Fi network, the victim should change the password to prevent them having further access. If they don't know how to do this, they can contact their internet service provider (such as BT, Virgin Media, TalkTalk, Vodafone or Sky) and their support staff will talk them through it.

Additional Steps for Wi-Fi Security

- Change all Wi-Fi passwords, including the SSID and router admin password, after leaving the relationship.
- If unsure how to do this, victims can contact their internet service provider (e.g., BT, Virgin Media, Sky) for step-by-step guidance.
- If home Wi-Fi is compromised, using mobile data (4G/5G) is safer, though it may incur extra costs.

Changing your internet router settings

Nearly all home routers provided by your internet service provider can be accessed using a web browser. An abuser could remotely modify various settings of the router, including changing the Wi-Fi password, or creating rules which would allow them to gain remote access to the victim's network.

Whilst home routers require a username and password to log into, they are often set up with a 'default' login and password, and so can easily be found out. Victims should change the default password on their home router, and turn of the setting that allows it to be accessed over the internet.

- BT: How can I set up or change the admin password on my BT Hub?
- Virgin Media: Hub's Wi-Fi name and password
- Sky: Find, change or reset your hub password

If victims need help doing this, they can contact their internet service provider who can talk them through the process. We've provided the help desk numbers of major internet service providers below.

- **BT** 0800 111 4567
- **PlusNet** 0800 432 0200
- **EE** 07953 966 250
- **Sky Broadband** 03442 411 653
- **Virgin Media** 0345 454 1111
- **Talk Talk** 0345 172 0088
- **Vodafone UK** 08080 034 515

- **Shell Energy** 0330 094 5801
- **Glide Student** 0333 123 0115
- **Zen Internet** 01706 902001
- **Ask4** 0114 303 3200
- **KCOM** 01482 602 555

Securing smart devices and IoT risks

Smart devices and IoT (Internet of Things) technology are increasingly common in homes and can be exploited by abusers for surveillance and coercive control. This section provides practical, device-specific advice to help practitioners support victims in regaining control of their digital environment. Consider the victim's safety before implementing changes, as actions like resetting devices or changing passwords may alert the abuser and escalate risk.

Securing Smart Devices and IoT Risks

Key Risks and Actions

- Video Doorbells & Cameras: Can record and stream activity remotely. If installed by an abuser, perform a factory reset, create a new account, change passwords, and enable two-step verification (2SV). Check for hidden cameras; some may not appear on the router if using mobile data.
- Smart Locks: Abusers can lock victims in/out or monitor door activity. Reset the system, set new PIN/passwords, or replace with a standard lock if control cannot be regained.
- Smart Speakers & Home Hubs: Voice commands and history are stored in linked accounts. Reset devices and accounts; use strong passwords and enable 2SV.
- Thermostats & Lighting: Can be used for coercive control (e.g. altering temperature or lights remotely). Reset and secure accounts after abuser leaves.
- Other IoT Devices: Includes fridges, kettles, TVs, plugs, and covert cameras in household items. Change all device and router passwords; disconnect non-essential devices from the internet.
- Bluetooth Headphones (Live Listen): Some Apple devices allow remote listening via paired headphones. Be aware of this feature during sensitive conversations.

General Advice

- Perform factory resets on all smart devices.
- Use strong, unique passwords and enable two-step verification (2SV).
- Consider disconnecting devices from the internet if not essential.
- Inspect household items for hidden cameras or microphones, report suspicious devices to police.

Refer to the vendor website for specific instructions.

Deleting the search history from smart devices

For some smart devices in the home, the search history can be deleted through the associated online account. Victims can access the account within the app (or a browser) using the links below. Deleted voice command requests will remove the audio recordings but maintains the transcripts for 30 days.

- My Google Activity
- Review your Alexa voice history
- Smart devices: using them safely in your home (NCSC guidance)

Gas and electricity 'smart meters'

Smart meters are **not** linked to home wi-fi networks, and only communicate directly with energy providers to take readings. The energy provider effectively owns (and manages) the smart meter, and will have safeguards in place to ensure that they can't be accessed remotely by another person. If an abuser was to tamper with the meter physically, it would be very difficult for them to make any changes without the company being notified.

Vehicle tracking

If an abuser and a victim use the same car, then the victim may want to remove the history of visited destinations that will be stored within the car's built-in satnav. Check the car's manual (or manufacturer's website) for details of how to do this. If the victim uses a separate mapping tool (for example Google Maps), then an abuser with access to their Google account will also be able to view a list of recent places.

Manage your Maps activity - Android - Google Maps Help

Delete recent directions in Maps on iPhone

In addition to built-in satnav, newer cars have companion apps that allow you to use a phone to track the vehicle's location, and to manage certain features. If an abuser has your account details (or access to your phone), they could track the location of your car, lock/unlock it remotely, and even activate some features (such as setting the heating). The NCSC guidance about how to recover online accounts if they've been hacked can help, or use the following vendor-specific links.

- How to use remote features with FordPass connect
- Add your car key to Apple Wallet on your iPhone or Apple Watch - Apple Support (UK)

Victims may also want to speak to their car dealerships or a mechanic about 'sweeping' the car for tracking devices that an attacker may have attached to the car to monitor it remotely.

Bluetooth Trackers (Air Tags, Tile, etc.)

Bluetooth trackers are small devices designed to help locate lost items, but they can be misused for stalking. Common examples include Apple Air Tags and Tile trackers.

How they work

- Air Tags use Apple's *Find My* network, leveraging nearby Apple devices to relay location data.
- Other trackers (such as Tile) use Bluetooth and sometimes GPS for location updates.

Risks

- Trackers can be hidden in bags, vehicles, or personal items without the victim's knowledge.
- They allow an abuser to monitor movements discreetly.

Signs of tracking

- Apple devices may display alerts such as *"Air Tag Found Moving With You"* (requires iOS 14.5 or later).
- Air Tags emit a sound after 8–24 hours away from their owner, but this can be tampered with.
- Android users can use Apple's Tracker Detect app to scan for Air Tags manually.

What to do

- If you find an unknown tracker:
    - Photograph it and note the time/date.
    - Avoid taking it to a safe location (such as home or refuge).
    - Contact the police or your case officer.
- To disable an Air Tag:
    - Remove the battery after recording its serial number.
    - Be cautious, disabling alerts the owner.
- Do not contact the tracker's owner directly.

For more details, refer to What to do if you receive an alert that an Air Tag, set of AirPods, Find My network accessory or compatible Bluetooth location-tracking device is with you.

Preventative measures

This section suggests steps victims can take to reduce the likelihood of an abuser being able to control or monitor their devices and accounts.

Creating strong passwords

Since many of us rely on passwords to control who can access to our devices and our important web services (such as social media accounts, email and banking), it's important that they are strong and difficult for someone to guess.

The longer and more unusual a password is, the harder it is for an abuser to guess it. Victims should:

- avoid using predictable passwords (such as dates, family and pet names)
- avoid the most common passwords that abusers can easily guess (like 123456 or passw0rd)
- avoid using the same password for different accounts (for example, to access email and to unlock a device)
- avoid using 'single sign on' (which is when you log into Facebook - or another service - using your Google details)
- take care when providing 'security questions' that can be used to reset passwords (such as 'what road did you grow up in?'); they should make sure they chose an answer that the abuser will not know

Victims can create a memorable password (that's also hard for an abuser to guess) by combining Three random words to create a single password (for example CupFishBiro). They can also write down their passwords if they need to (provided they keep them somewhere safe and not known to the attacker).

Note: When logging into online accounts, most web browsers (such as Chrome and Safari) will offer to save them for you. Normally, the NCSC would recommend that users do this. However, since abusers may have access to the device, we recommend that victims do not do this.

Take special care of email passwords

Victims should use a strong and unique password for their email account (that is, one that they don't use for any other account). If an abuser gets access to a victim's email account, they could:

- reset all their other account passwords (and get access to **all** their other online accounts)
- access private information about them (including banking details)
- post emails and messages pretending to be from them (and use this to trick other people)

If victims have re-used their email password across other accounts, they should change it as soon as possible.

Keep your devices updated

Victims should always install updates for their devices and apps (including for antivirus products) as soon as these are available. This helps to keep devices secure. They should also switch on the option to install automatic updates (if available).

Antivirus and Malware Protection

For laptops and PCs:

- Ensure built-in antivirus (Windows Defender or macOS XProtect) is enabled.
- Run a scan on the old device before transferring data to a new one.
- Run a scan on the new device after migration to ensure it's clean.
- Schedule regular scans for ongoing protection.

For more details, see NCSC's What is an antivirus product? Do I need one?

Add extra security by setting up 2SV

Many online accounts and services allow victims to set up two step verification (2SV), also known as two-factor authentication (2FA) for first use which means that even if an abuser knows the victim's password, they won't be able to access their accounts. It usually works by sending you a PIN or code (often sent by SMS), which you'll then have to enter to prove that it's really you. If victims are given the option, it's worth taking the time to set up 2SV on important accounts like email and banking, even if these are already protected using a strong password. It only takes a few minutes, and they're much safer as a result.

Note that:

- once they've set up 2SV, they won't have to enter the PIN or code every time they use a service (most accounts will only prompt you to enter the PIN when it detects an 'unusual' login, such as from a different device, or from a device that you've not used in a long time)
- they don't necessarily need a mobile phone to set up 2SV; some organisations will let you use a landline number, or physical token (such as a card reader for online banking)
- *any* type of 2SV is better than not having it at all, so encourage victims to check their provider's website to see what methods they support

Warning: If the abuser has access to the device that is being used for 2SV (for example, if the abuser has access to the victim's phone that receives a 2SV PIN code), then 2SV won't provide additional protection.

Make sure stolen devices can be tracked, locked and wiped

If an abuser steals their victim's phone (or other device), there's a range of invaluable tools available to the victim, **provided these have been set up in advance**. These free web-based tools can be used to:

- track the location of a device
- remotely lock access to the device (to prevent anyone else using it)

- remotely erase the data stored on the device
- retrieve a backup of data stored on the device

Victims will need to log into their Google or iCloud accounts. Note that if **location tracking has been turned off**, these functions won't work.

- Find, secure, or erase a lost Android device - Google Account Help.
- Erase a device in Find Devices on iCloud.com - Apple Support (UK).

App Protection and Privacy Settings

Victims can take steps to make it harder for an abuser to monitor messages or access apps. These measures complement device security guidance in existing sections such as Securing victims' devices, Changing passwords, and Preventative measures.

Hide Message Notifications and Previews

- Turn off message previews on the lock screen so content is not visible without unlocking the device.
- iPhone: Settings → Notifications → Show Previews Stop, mute, and change message notifications on iPhone
- Android: Settings → Notifications → Hide sensitive content Control notifications on Android - Android Help
- Consider disabling notifications or setting the phone to silent to avoid drawing attention.

Manage App-Specific Privacy Settings

- Review privacy settings in messaging apps (e.g., WhatsApp, iMessage):
    - Control who sees your profile photo, status, and last seen.
    - Disable read receipts if safe to do so.
    - Use disappearing messages cautiously, previews or forwarded messages may persist.
    - Check for linked devices in apps like WhatsApp and remove any you do not recognise.

Deleting Messages, Photos and Videos

- Deleted items often remain in "Recently Deleted" or "Recycle Bin" for 30 days—remove them from these folders.
- Be aware that gaps in conversations or missing media may raise suspicion.

Third-Party Tracking Apps

- Uninstall or disable any apps that share your location or track your activity if you suspect misuse.
- For detailed instructions, see:
    - Apple Personal Safety Guide
    - Google Account Safety
    - WhatsApp Safety

Using Public Wi-Fi Safely

When away from home, victims may need to use public Wi-Fi. To reduce risks:

- Verify the network name matches what is displayed on the premises.
- Check websites start with https and look for the padlock symbol (secure connection).
- Consider having the device "forget" the Wi-Fi after leaving the area to prevent automatic reconnection.
    - Connect to Wi-Fi networks on your Android device
    - How to forget a Wi-Fi network on iPhone, iPad, Mac or Apple Vision Pro

VPN Use and Limitations

A VPN can hide browsing details and IP addresses when using Wi-Fi, but:

- It does not make insecure websites safe, avoid sites without HTTPS.
- If the abuser has access to the Wi-Fi network, they already know the victim's location.
- VPNs may help if the abuser monitors online activity via shared accounts, but using mobile data is often safer.
- Many VPNs are paid services; free ones can have restrictions or security issues.