National Cyber Security Centre
a part of GCHQ

Domestic cyber crime

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

Contents

Introduction

This guidance has been produced to support practitioners working with victims of domestic 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 enquiries@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 you suspect 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 Twitter
- Location based features in LinkedIn

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.

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: How Can I Keep My Stats Private?
- Apple Watch: Share your Activity and compete with friends with your Apple Watch (stop sharing section is halfway down the page)

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

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.

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.

.

Using video conferencing safely

Since the COVID-19 pandemic, 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's Duo), 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, Skype, Houseparty 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.

- Manage family sharing on an iPhone/iPad device (Apple phones and tablets).
- Manage family sharing on an Android device (such as those manufactured by Google, Huawei and Samsung).

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-factor authentication, 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 site data in Firefox
- Remove website data in Safari on Mac
- Clear browsing data from Google Chrome
- 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.

- Delete your Google Chrome browsing history
- Managing your yahoo! search history
- 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
- Twitter: help with my hacked account
- I think my Instagram account has been hacked
- Snapchat: my account is hacked
- LinkedIn: Reporting a compromised account
- Reddit: I need help with a hacked or compromised account
- Tinder: I think my account has been compromised
- 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 use two-factor authentication (2FA). You should always set this up, as it adds extra security to your online banking.

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.

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

If an abuser knows the victim's login details, they can remotely access an increasing range of 'smart' devices. Smart devices are any household gadgets that connect to the internet, so not just TVs, speakers and doorbells but also CCTV cameras, 'nanny cams', smart locks, smart lightbulbs and smart thermostats. The most common examples of abuse include:

- monitoring activity in the house (smart cameras)
- listening to conversations (smart speakers and smart cameras)
- detecting when someone leaves the house (smart doorbells)
- changing the temperature (smart thermostats)
- turning lights on and off (smart light bulbs)
- turning power sources on and off (smart plugs)
- playing music (smart speakers)
- preventing someone from entering or leaving the house (smart locks)

Changing the user name and using a strong password for each of these makes it harder for an abuser to access smart devices remotely. If the online account for the device has two-factor authentication (2FA) available, this should be turned on to provide extra protection.

Victims should consider resetting all smart devices in their home, even if they're not sure they're currently being monitored by the abuser. Resetting the router's Wi-Fi password can help here, as devices that are linked to the router via Wi-Fi can't be controlled by the abuser if they don't know the new router password.

If victims can't access the account that controls the smart device (but they still need to use it), they can check to see if there's an option to 'reset' the device (for example by pressing a button). This will usually remove the abuser's account. Note that each smart device is different, so check the support area of the manufacturer's website for details of how this works. Below we've listed relevant pages for some of the most common smart devices.

- Google Home: managing devices in the Home app
- Alexa profile settings
- Yale Smart Locks: setting access levels
- Ultraloq Smart Locks: managing users

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.

- Delete directions and places from your Google Maps history
- 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
- Use your iPhone or Apple Watch as a car key

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.

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).

Add extra security by setting up 2FA

Many online accounts and services allow victims to set up two-factor authentication (2FA), 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 2FA 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 2FA, 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 2FA; some organisations will let you use a landline number, or physical token (such as a card reader for online banking)
- *any* type of 2FA 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 2FA (for example, if the abuser has access to the victim's phone that receives a 2FA PIN code), then 2FA 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, lock or erase a lost Android device.
- Erase an iPhone/iPod device.