National Cyber Security Centre
a part of GCHQ

Domestic abuse and stalking: cyber security guidance for practitioners

This guidance has been written to support advocates and practitioners working with victims of domestic abuse and stalking. It aims to provide actionable advice which practitioners can use with their clients.

While the guidance contains up to date technical advice, it does not make any attempt to assess the risk of providing this guidance to victims. Practitioners and advocates should consider the individual circumstances of each person they are working with, in particular whether following the advice could put the victim in greater danger.

We will continue to update this guidance in line with feedback from practitioners and advocates, and in line with changes to technology. Please send any feedback to charity.engagement@ncsc.gov.uk .

In this guidance:

1. Being tracked by an abuser

How can I prevent being tracked through my mobile device (smartphone, tablet)?

There are some simple steps you can take to make it more difficult for someone to track you through your devices or online. If the abuser has physical access to the device, you should prevent them from being able to access it by using passwords and/or biometric authentication (fingerprint or 'face ID');

- How to set a passcode on an iPhone/iPad.
- How to set a passcode on Android devices.

It's important to change your passwords, especially if you think the abuser knows them. If the abuser previously had access to the device through biometric authentication, you should ensure that their credentials (their fingerprint or face record) are removed within the settings of the device and only your fingerprint/face can unlock the device.

- How to change credentials on an iPhone/iPad.
- How to change credentials on Android devices.

However, you should be mindful of changing your credentials as this will most likely become apparent to your abuser.

Many social media platforms such as Twitter, Instagram and Facebook use geotagging to show your friends and followers where you posted the photo or message from, which your abuser would also be able to see. Therefore, turning off location settings on any social media apps using the links for major platforms above would be advisable.

How could an abuser be tracking my mobile device (smartphone, tablet) and how can I remove tracking software?

Tracking could be done by a range of different methods. It could be as simple as accessing your location through an application (app) such as *Find Friends*, *Snapchat* or a similar app that has location services switched on. In settings, you can review which apps have location services switched on. This should be turned off if you believe an app could be being used to track you. Alternatively, depending on the device, you may be able to turn off access to location information for all apps.

- How to turn off location services on an iPhone/iPad.
- How to turn off location services on Android devices.

It should be noted that some apps specifically require access to a user's location to work; so disabling location features could limit functionality.

Alternatively, the abuser may have installed malicious software (malware) on your device to be able to track you without your knowledge. Such malware can be bought online relatively easily so the abuser wouldn't need much technical knowledge to be able to do this. Examples include FlexiSpy and WebWatcher. Malware of this kind is not normally illegal and is often advertised as things like 'parental control' or 'employee monitoring' software but it can be used for malicious purposes to track people.

There is **no reason to get rid of the device** if you believe there is tracking malware on it. Generally, we would advise that any apps that you don't think you've installed yourself should be deleted.

- How to delete apps on an iPhone/iPad.
- How to delete apps on Android devices.

Sometimes tracking malware can be installed on your device by your abuser but you cannot see it. If you suspect that your abuser is tracking you by your device but cannot see any apps that might be doing this, then you should consider resetting the device to factory settings which should remove it. See the NCSC's factory reset guidance for more information on how to do this without losing other information on your device that you want to keep like your photos.

It should be noted that if you remove applications or reset the device, the abuser responsible for adding the malware or the tracking app on your device will likely be alerted. They may however not be able to confirm that you are responsible for removing it.

I have to use video calls so my children can talk to their parent (who is an abuser), could they determine my location from this?

Most video call software (e.g.- Skype, FaceTime) provides a connection between participants over the internet using Internet Protocol (IP). It is possible that an abuser could find out your IP address and then identify an approximate location from that (e.g. nearest town). However, this isn't always accurate and your IP address will change from time to time making locating you via this method more difficult. If you are concerned about this then you can instead make video calls over your phone's mobile network using 3G/4G rather than wi-fi as this will make it much harder to identify your location from your IP address. Note that your mobile phone itself can still be tracked by an abuser, please refer to section 1 above.

You can also take precautions when having your video calls to ensure no items in the background indicate your location. You may also want to consider making video calls away from your home or a sensitive location, such as a refuge.

You should be aware it is impossible to prevent a screenshot or image being taken during a video call, although some applications may notify users if a screenshot has been taken.

2. Unauthorised access to your device(s)

Can a device be hacked if the abuser has never had it in their possession?

Your device could be hacked without it being in the possession of the abuser. However, this is relatively difficult to do without specialist knowledge and is unlikely in most cases.

A device can be compromised by a range of different methods, but receiving a phishing email urging you to visit a website or open an attachment is the most likely. The NCSC has some easy to follow tips for spotting a phishing email and what to do if you suspect an email isn't genuine. Other ways in which a device can be hacked are by visiting a malicious webpage or downloading and installing malicious code bundled with other software. To help protect from this, you should ensure that your device has the latest versions of software installed and that PCs and laptops are running an updated antivirus product.

What should I do if I believe my device or an online account has been hacked?

There is no definitive way to know that you have been hacked. However, indications that your device or an online account may have been hacked include:

- Your device running slowly, rebooting itself, frequently closing programmes or apps you are using, or opening those you are not
- Your device is presenting pop-up boxes from programmes/apps you don't recognise asking you to do unexpected things
- Someone you know tells you that they've received unexpected messages from you, which are out of character or advertising unlikely products, or perhaps asking for money.

If you believe you have been hacked, you should collect any evidence on your device if it is safe to do so and report it to Action Fraud. This is the police's national reporting centre for fraud and cyber crime.

If you think an online account (e.g. email or social media) has been hacked, the NCSC provides a step by step guide to recovering an account.

If you think your device has been hacked, this will usually include the installation of malicious software. If you believe there is malicious software on your device, then you can follow our guidance which will help you remove it. Below are links to guidance on resetting the most common types of device to factory settings which should remove the malicious software.

- Apple iOS (iPhone/iPad): https://support.apple.com/en-gb/HT201252
- Google Android: https://support.google.com/android/answer/6088915?hl=en-GB
- Windows PC/laptop: https://support.microsoft.com/en-us/help/17085/windows-8-restore-refresh-reset-pc
- Apple mac https://support.apple.com/en-gb/HT208496

3. Unauthorised access to your online accounts

How can I stop an abuser using my bank accounts to track where I have been?

If you have a joint account with an abuser, you will be unable to prevent them seeing the locations that payments have been made as they have equal access to the account. If you do not want the abuser to see this information, then you can open your own account in just your name. If this is not possible and your abuser has access to your account where they can view the locations of your payments, change your password and login credentials (e.g. PIN number and memorable information) with your bank.

Most banks give you the option to use two-factor authentication (2FA), turning this on will ensure an abuser can't access your account even if they know/guess your password/PIN. 2FA adds extra security when you login to your online accounts. It confirms a login is genuine through a second device. For example, by a code that is sent to your phone.

Remember that location information is also included in your bank statements. If the abuser is checking your paper statements, then you can switch to paperless statements. Alternatively, if none of the above is possible then you may want to consider paying for products with cash.

If my social media account has been hacked or unlawfully being used by someone else, is there any support I can get from these sites?

As well as referring to NCSC's guidance to recovering an online account if it has been hacked, social media providers also provide their own advice. If you have lost access to or control over a social media account, then your service provider can also help. Once you have confirmed your identity, it is relatively easy to change your password for a social media account. Where possible we also recommend enabling two-factor authentication (2FA) by following our guidance. 2FA adds extra security to your online accounts. It confirms a login is genuine through a second device. For example, by a code that is sent to your phone. You'll be more secure if you set up 2FA on all your important accounts such as email, online shopping as well as social media.

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

- Facebook: https://www.facebook.com/hacked
- Twitter: https://help.twitter.com/en/safety-and-security/twitter-account-hacked
- Instagram: https://help.instagram.com/149494825257596
- Snapchat: https://support.snapchat.com/en-GB/a/hacked-howto
- LinkedIn: https://www.linkedin.com/help/linkedin/answer/56363/reporting-a-hacked-account?lang=en
- Reddit: https://www.reddithelp.com/en/submit-request/account-issues
- Tinder: https://www.help.tinder.com/hc/en-us/articles/115005149706-I-think-my-account-has-been-hacked-

Furthermore, if you receive emails from your social media provider indicating an attempted log in from an unknown device, this could indicate someone is trying to hack your account. Many social media sites have a feature that enables you to view the devices you are logged into your account from and sign out of any you don't recognise.

Additionally, if someone is pretending to be you on a social media platform, you should report the account to the provider and request that the fake account be shut down.

How do I stop an abuser accessing my photos and videos that are stored on the cloud?

A lot of the information stored on your devices, such as photos, videos and documents are often backed up to the cloud, helping ensure you have a copy if you lose your device. You should ensure that you are using a strong password (such as 3 genuinely random words that can't be easily guessed) to access your cloud accounts and ensure you change your password if your abuser has had access to them in the past. Alongside this, turning on two-factor-authentication will give you an added layer of security.

Many cloud providers allow users to share photos, videos, documents etc with other users and often have Family Sharing settings turned on by default, for example *Apple* offer this feature with *iCloud*. Where possible, you should disable this feature by following this guidance from Apple.

Furthermore, ensuring these security measures have been enabled will limit the chances an abuser is able to access any sensitive images that could be used in revenge against you by sharing with other people – commonly known as "revenge porn".

My device has been taken by the abuser, can I log out of my accounts or restrict access remotely?

If your device (smartphone, tablet, laptop) is taken by your abuser, there are several things you can do to prevent them gaining access to the device and any information stored on it or accounts you're logged in to on it. Some platforms such as Facebook or Instagram allow you to sign out from another device. Once you've done this you should then change your password so they can't log back into your account. You should also be able to remotely lock or wipe the stolen device. You will need to log into to your Google account or iCloud account to do this.

4. The security of internet-connected devices in the home

Could an abuser access the smart devices in my home (such as a smart speaker, thermostat, security camera and doorbell) and use them to abuse me?

Accessing smart devices remotely is usually only possible if the abuser knows the login credentials (e.g. password) for the device. By logging into the device remotely they could change the temperature on the thermostat, play music remotely or access a security camera with a microphone for example to listen in to your conversations. Changing the login credentials for the device should prevent them from accessing it remotely. If the online account for the device has two-factor authentication available, this should be turned on to prevent your abuser being able to access the device remotely even if they guess your new password.

If you cannot access the online account for a smart device but it is still in your home and you need to continue to use it, where possible, the device should be reset to remove the abusers account that is associated with it. Some devices may be able to be reset by a physical button, although each device is different, so you should refer to the manual or online support for these.

One concern may be that your smart speaker is eavesdropping on your conversations. If this is the case, you should be able to remove the user from the smart speaker's online account. Here is some guidance on how to do this for some of the most popular smart speakers - Amazon Alexa and Google Home .

Can an abuser gain access to the webcam or microphone on my device and what can I do to stop this?

When you are not using your webcam, one quick and simple solution is to stick a piece of dark tape or a webcam cover over the lens, so even if someone does have access to your webcam they will not be able to see anything from it. You can also choose to turn off the webcam and the microphone in the device settings. As above, to help protect you from someone gaining access, you should ensure that your device always has the latest versions of software installed and that computers and laptops are running an updated antivirus product.

How can I delete search history on my devices; including internet-connected devices in the home such as smart speakers?

The majority of internet browsers (e.g. Google Chrome, Apple Safari, Microsoft Internet Explorer, Mozilla Firefox) offer a private search option (known as Incognito Window in Google and InPrivate Window in Microsoft), when browsing the web. Using this does not save browsing history, prevents passwords being saved, and only saves information temporarily while the browser is open.

To delete search history, cookies and other temporary files from your browser, go to the settings menu, here are instructions to do this in Chrome, Internet Explorer, Safari and Firefox. Additionally, if you have an associated online account (e.g. Gmail account or Microsoft account), you should delete your search history by logging into it. Furthermore, you can disable this feature so your browser search history will not sync with your associated online account. The main browser and internet search providers have guidance online which will help you to do this. Here are links to the guidance from Google, Yahoo, and Bing.

For some internet-connected devices in the home e.g. Google Home and Amazon Alexa, search history can be deleted through your associated online account. You can access the account within the app or browser using the links provided.

Are smart meters secure, could they be accessed remotely or tampered with?

Smart meters are not linked to your home wifi network and only communicate directly with your energy provider to send them your energy readings. The owners of the meter is your energy provider, who will have security measures in place to ensure that the meter cannot be accessed remotely by another person. Furthermore, if an individual was to tamper with the meter physically, it would be very difficult for them to make any changes without the company being notified or made aware. Overall, the hacking of smart meters by an abuser is unlikely.

Could an abuser be tracking me using my car's built in sat nav?

Some of the latest cars have companion apps that can track their location. It is possible that an abuser could be tracking the location of your car and know where you are going. If this is an issue you should speak with the dealership or a mechanic and discuss the options of having the abuser removed from the online account and tracking ability switched to your device instead.

5. Wi-Fi and landline security

How can I make sure my Wi-Fi is secure and could my abuser access it without being inside my home?

It is possible to access your Wi-Fi network without access to your home as the signal is likely to extend beyond the property. This means that an abuser could access the Wi-Fi network from the road outside your home, without having to be physically present within your property. Furthermore, there is widely available software which can be downloaded for free to analyse what websites people using the Wi-Fi network are visiting. If the abuser has previously had access to your Wi-Fi network, you should ensure a password is required to access it and that this password is changed to prevent them having further access. If you don't know how to do this, you can contact your Internet Service Provider (such as BT, Virgin Media, Sky) via their helpdesk and they should be able to talk you through changing it.

Could my abuser change settings or monitor my Wi-Fi remotely?

Nearly all home routers provided by your Internet Service Provider (BT, Virgin Media, Shy etc) can be accessed using a web browser (e.g. Google Chrome, Microsoft Internet Explorer) once connected to the Wi-Fi network. Access to this could allow an abuser to modify various settings of the router, including creating rules which would allow them to gain remote access to your network. Whilst home routers require a username and password to log in, they can be easily guessed or found on the internet because they are set up in the same way for all customers. We therefore recommend changing the password for your home router and disabling the ability to access it over the Internet. Again, if you don't know how to do this, you can contact your internet service provider via their helpdesk and they should be able to talk you through changing this.

Can my landline be tapped?

It is unlikely that your landline has been tapped so someone else can listen to your calls. However, if you believe it has been tapped you should contact the police on 101 for them to investigate. If you have access to a mobile phone you may choose to use this instead.