Phone numbers, home Wi-Fi and public Wi-Fi

Hiding your phone number

A victim of abuse may need to call their abuser, for example to arrange child visits with an ex-partner.

Landline phones

Landline numbers can be hidden from public directories by becoming **ex-directory**. This means a person can have themselves removed from the Phone Book and will not be available via BT 118500 Directory Enquiries, nor via the online directory service.

When ringing outward from a landline, the number can be hidden by dialling **141** in front of the main number and then dialling. It is also possible to arrange to have the number with withheld on all calls. How do I withhold my telephone number?

A victim of abuse will need to do **both** these things to keep their landline number private.

Mobile phones

Mobile phone numbers can also be hidden when dialling out so that the caller's number information is hidden. Dialling **141** before the phone number should make the call appear as No caller ID, Unknown, or similar. Check before using that this will work for your phone provider.

Many phones will allow caller ID to be blocked for all calls - e.g. via Settings > Phone or in the settings of the phone app on Android.

Incoming calls

If an abuser is blocking their own caller ID when calling the victim, it will be more difficult for the victim to report them. Where a victim is building a case against an abuser, they should note the time and date of any such calls, and report to police. This may allow the police to track the call.

You can choose to block unknown callers on both mobile and landline. **Note:** if you block withheld numbers you risk blocking legitimate calls where the number is withheld - it is quite common for GP surgeries, hospitals etc to withhold their number on outgoing calls.

Example services (check your provider/handset for exact details) include:

- iPhone - Settings > Phone > Silence Unknown Callers. This will silence and send straight to voicemail any calls from withheld numbers, as well as numbers that you've never been in contact with, don't have saved in your contacts list and haven't received their number another type of way, such as through emails. Silenced calls will appear in your call log, and in voicemail if the caller leaves a message. If you make an emergency call this setting will be suspended for 24 hours.
- Android - Phone > Settings > Blocked numbers > Unknown. This will silence and send straight to voicemail any calls from withheld numbers. The call will appear in your call log, and in voicemail if the caller leaves a message.
- BT landline - BT Call Protect is a free service that sends certain kinds of call to junk voicemail. It includes the option to block withheld and/or unrecognised numbers – BT Call Protect – 'How to…' guide

Intercepting calls and online activity

Can my mobile by intercepted?

Common stalkerware apps can also record conversations on mobile devices. If the victim is concerned they may have such an app on their phone, they can follow the guidance in New and Second-hand Devices to reset the device (doing a manual transfer of apps to reinstall only ones they want, rather than anything that may have been installed without their knowledge).

For sensitive calls, they may wish to use another trusted mobile phone or landline - one that the abuser should not have been able to interfere with, such as a friend's mobile or a landline in their workplace.

Can my landline be intercepted?

It is unlikely that a landline would be 'tapped' - that is, intercepted remotely allowing the abuser to listen in on calls. However, if a victim of abuse believes it

has been tapped they should contact the police on 101 for them to investigate. If they have access to a mobile phone they may choose to use that instead.

If the abuser has, or has had, access to the home they could install an in-line recording device - the example on the right looks like a normal ADSL filter. Again, if a victim of abuse believes their calls are being intercepted they should contact the police.

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 someone's Wi-Fi network without access to their home as the signal is likely to extend beyond the property. This means that an abuser could access the Wi-Fi network remotely from the road outside their victim's home, without having to be physically present within the property.

If the victim has left the relationship, they should change all passwords for the Wi-Fi, including the administration passwords and the SSID. This will ensure the abuser can no longer access the Wi-Fi using previous passwords. If they don't know how to do this, they can search online for instructions, or contact their Internet Service Provider (e.g. BT, Virgin Media, Sky) via their helpdesk and they should be able to talk them through changing it.

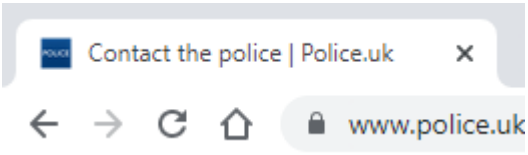
Using mobile data (4G or 5G)

If the victim believes their home Wi-Fi is compromised, using mobile data will be a more secure option. However this will require the victim being able to afford enough data to fit their needs. High data charges may also arouse the abuser's suspicious, if they see the bill.

Using public Wi-Fi

When away from home a victim may want to connect to public Wi-Fi as an alternative to using mobile data. The chances of an abuser intercepting Wi-Fi traffic is low; however anyone using public Wi-Fi, e.g. that available in a cafe, shop or on public transport, should:

- Check that the Wi-Fi is the correct service - that it matches any details displayed on the premises, that it is not one of several similar-looking networks available.
- Check that any website that requires personal details to be input is secure - by checking it starts https (rather than http) or by looking for the padlock symbol. **Note:** The padlock indicates a secure connection between the browser and the website, it does *not* mean that the site is legitimate.



- Consider having the device 'forget' the Wi-Fi once they have left the area. If they do not 'forget' the Wi-Fi their device will join automatically next time they are in range, which could reveal to an abuser that they've used it before.
    - Android: https://support.google.com/android/answer/9075847?hl=en-GBApple
    - Apple: https://support.apple.com/en-gb/HT208941

Virtual Private Networks (VPNs)

A VPN will hide certain things that would otherwise be visible to someone with access to the Wi-Fi someone is using – that could include home Wi-Fi if the abuser has admin access; unsecured public Wi-Fi; or 'public Wi-Fi' that's actually been spoofed by the abuser.

A VPN will hide:

- The *detail* of what someone doing on an **unsecure** website. The answer here is not to use unsecure websites (look for the padlock).
- *Basic* information on what a person is doing online – what websites they are visiting. If just knowing what website the victim is visiting would cause an issue with the abuser, the victim should try to use 3/4/5G for this purpose.
- The IP address in use, thus helping to hide where a person is. However if an abuser has access to the Wi-Fi, whether at home or elsewhere, they will already know where the victim is.

- Information if the abuser has access to an account belonging to the victim – in particular some services show the IP address of where the person last connected from, which could reveal their movements. Again if this is a concern, try to use 3/4/5G instead of Wi-Fi.

A VPN is therefore only of use to a victim of domestic abuse if their abuser has access to the Wi-Fi they are using, and they are doing very specific things online (that they can probably avoid doing over Wi-Fi). They also require some assessment as to how secure and trustworthy they are, and many are paid services (free ones tend to come with restrictions or other issues).

All URLs

Becoming ex-directory: https://www.bt.com/help/landline/calling-features-and-security/how-do-i-sign-up-to-ex-directory-services-

How do I withhold my telephone number?
https://www.bt.com/help/landline/calling-features-and-security/how-do-i-withhold-my-telephone-number-

BT Call Protect – 'How to…' guide: https://www.bt.com/help/security/bt-call-protect----how-to-----guide

Forget a Wi-Fi network:

Android: https://support.google.com/android/answer/9075847?hl=en-GBApple

Apple: https://support.apple.com/en-gb/HT208941