DASSL
Domestic Abuse Support
Services Lancashire

How to cover your tracks online if you're experiencing domestic abuse

If you are experiencing domestic abuse, using the internet can be a lifeline for accessing support, gathering information, and making plans for your safety...

Unfortunately, abusers often use technology as a tool for control, monitoring your online activity to restrict your access to help or track your movements. It is crucial to know how to cover your tracks online to protect yourself from potential risks.

This article will guide you through practical steps to erase or hide your online activity, keeping in mind that every action may carry its own risks. Always make sure you assess your situation carefully and only take the steps you feel safe doing.

As a domestic abuse support service, we have the resources available to help you and we're always here if you need our support.

Clear your browsing history and cache

Abusers may check the history of websites you've visited, so regularly clearing your browsing history is essential.

Here's how to do it in **Google Chrome**, the most common browser.

1. Open Chrome and click on the three vertical dots (menu) in the top-right corner.
2. Select **History** > **History** again.
3. On the left, click **Clear browsing data**.
4. Set the **Time range** to cover the period you want (last hour, day, or all time).
5. Check the boxes for **Browsing history**, **Cookies and other site data**, and **Cached images and files**.

6. Click **Clear data**.

Use private browsing or 'incognito' mode

Whenever possible, use your browser's private browsing feature, which doesn't save your history, cookies, or search data after you close the window.

Here's how to do it on each browser.

- **Google Chrome**: Open Chrome, click the three dots in the top-right corner, and choose **New Incognito Window**.
- **Firefox**: Click the menu button and choose **New Private Window**.
- **Safari**: Go to **File** and select **New Private Window**.
- **Edge**: Click the menu button and choose **New InPrivate Window**.

Disable Cookies and auto-fill suggestions

Cookies track your activity on websites and store your login information. When you click on a webpage, you'll often get a pop-up asking to consent. However, disabling them reduces the chance of being tracked.

Here's how to block cookies on Chrome (it's also similar on most popular browsers).

Chrome:

1. Go to **Settings** > **Privacy and security**.
2. Click on **Cookies and other site data**.
3. Choose **Block all cookies** or adjust to your preference.

Regularly delete your search history

If you're logged into a Google account, your searches are stored in '**My Activity**'. You can delete this history:

1. Go to myactivity.google.com
2. Click on **Delete activity by**.
3. Select **All time** or specify a date range.
4. Choose **Delete**.

You can also pause your search history by going to **Data & Privacy** in your Google account and toggling off **Web & App Activity**.

Always be cautious with your emails

If your abuser has access to your email account, they might be able to see emails from helplines or support services. Use a separate, secure email account that they don't know about.

- Create a new account with a provider like Gmail or Yahoo, and don't save the password or login details on shared devices.
- If possible, use this account only on a secure device that your abuser does not have access to.

Clear your call and message history

If you've called hotlines or texted for help, make sure to clear your phone's call logs and message history:

- **Android**: Go to your **Phone** app, open **Call History**, select the numbers you want to erase, and tap **Delete**.
- **iPhone**: Open the **Phone** app, go to **Recents**, and swipe left on the calls you want to delete.

For text messages, open the conversation and delete it from your messaging app. If you're using messaging apps like WhatsApp, delete individual messages or conversations.

Use a safe device that only you have access to

If possible, use a device your abuser doesn't have access to. This could be a phone, computer, or tablet belonging to a trusted friend or family member, or a device at a library or community centre.

Familiarise yourself with safe exit from websites

If you are on a website and feel that your abuser may walk in or check on you, many support websites – such as SafeNet – have a **quick exit** or **escape button** that redirects you to a neutral page, like a weather report or search engine.

Make sure to familiarise yourself with where this button is when visiting support sites like domestic violence hotlines.

Avoid using location sharing

Ensure that apps like Google Maps, Find My iPhone, and social media do not share your location. It's quick and easy to disable your location services; here's how you do it:

- **Android**: Go to **Settings** > **Location**, and toggle off location tracking or adjust permissions for specific apps.
- **iPhone**: Go to **Settings** > **Privacy** > **Location Services** and turn it off or restrict individual apps.

Also, check apps like Facebook, Instagram, and Snapchat, as these may share your location in posts or stories.

Log out of social media accounts

If you share devices, always log out of social media accounts like Facebook, Instagram, or Twitter. Check for linked devices and deauthorise any that the abuser could have access to:

- For Facebook, go to Settings & Privacy > Security and Login, and review the devices that have logged into your account.
- For Instagram, go to Settings > Security > Login Activity.

Our final thoughts...

Your online safety is an important part of your overall safety plan. If you feel that covering your tracks may provoke your abuser, take steps that are less obvious, like using private browsing modes or safe devices.

Remember, clearing your digital footprints might not guarantee complete privacy, but these measures can help protect your online activity from being easily tracked.

If you are in immediate danger, call 999.