


# GUIDE TO ONLINE SAFETY FOR SURVIVORS

JUGNI



Technology and the internet can be a powerful resource(s) for survivors of domestic violence. They can provide access to essential information and link them to platforms in order to connect them with friends, family members, service providers and advocates, among others. Mobile apps such as Bright Sky (by Hestia, UK) and Hamqadam (by Shirkat Gah, Pakistan) have been developed to provide much needed assistance and emergency relief to survivors.

However, as much as technology can help facilitate a survivor's escape from abuse, it can also be used by abusers to initiate, continue and / or escalate the abuse. For survivors of domestic abuse, concerns can quickly arise regarding stalking, harassment, privacy invasion, impersonation, non-consensual sharing of images and / or videos, and other threats. This could leave many survivors feeling exposed and vulnerable online.

This is why - if you are in an abusive relationship, or know someone who is - it is essential to ensure your safety online (and that of those connected to you, who may be affected by the abuse).

If possible, try to avoid using shared laptops and / or cell phones when researching topics like legal options, transitional housing, travel plans and safety plans for you and your children. You can even use a Virtual Private Network (or VPN) to hide your IP address while you safely surf the internet for resources.

If you believe someone is monitoring your devices - and / or your activity online - we would recommend that you use caution when visiting online resources for survivors. You can either access these from a remote location (such as a cyber cafe) or use your browser's incognito mode. Be sure to clear your browser's history (both in your laptop / computer and your cell phone) after you are done. The way to delete your browser history is different for each browser. It will also be different depending on whether you are using your laptop/computer, or your cell phone.



## Clearing Browser History on Chrome.

1. When using your **laptop / computer**, you can clear your browser history by taking the following steps:

**1.1** Open the Chrome Browser.

**1.2** At the top right, click *more* (or click on the three (3) vertical dots).

**1.3** Click on History. A drop down menu will show you all the recent activity / history of your browser.

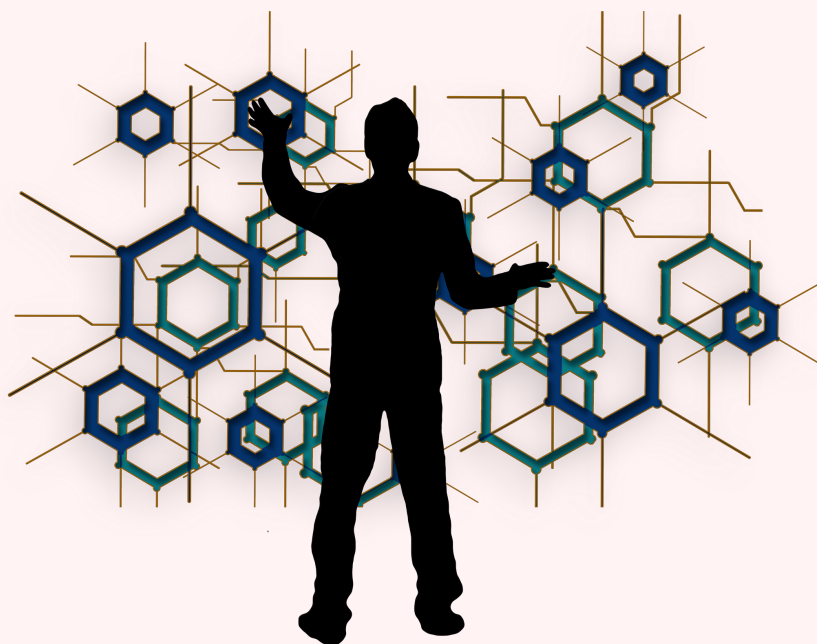
**1.4** On the top of the menu, the word History will be repeated. Click on that.

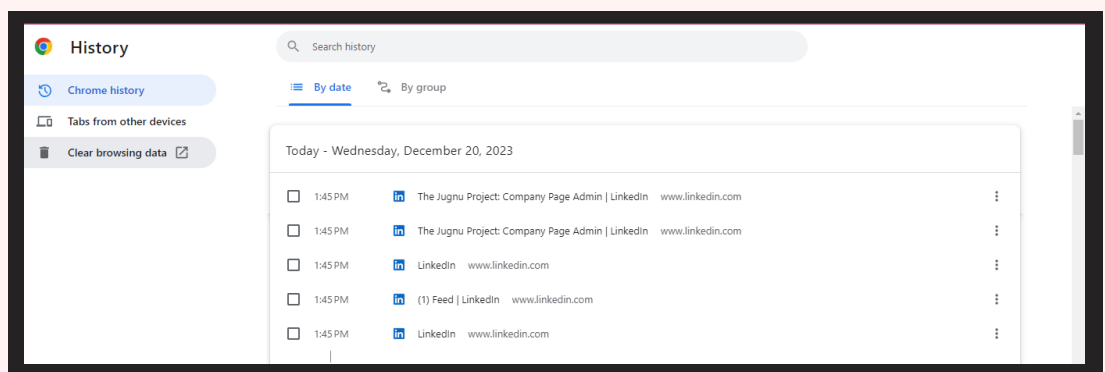
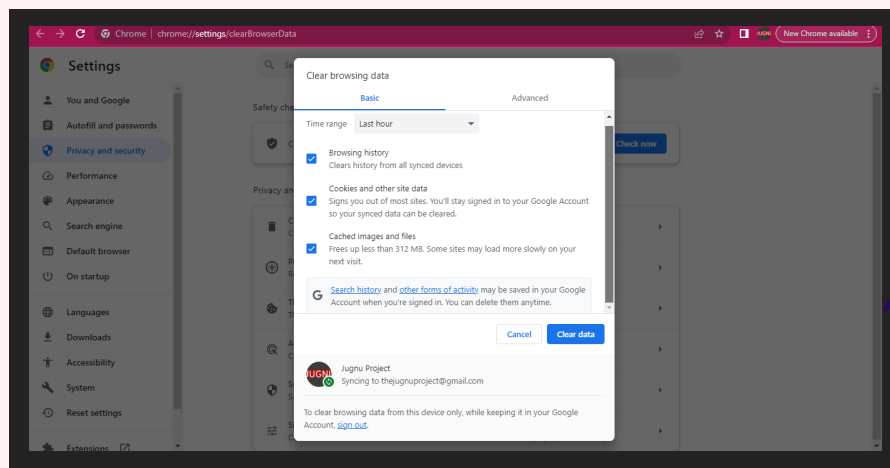
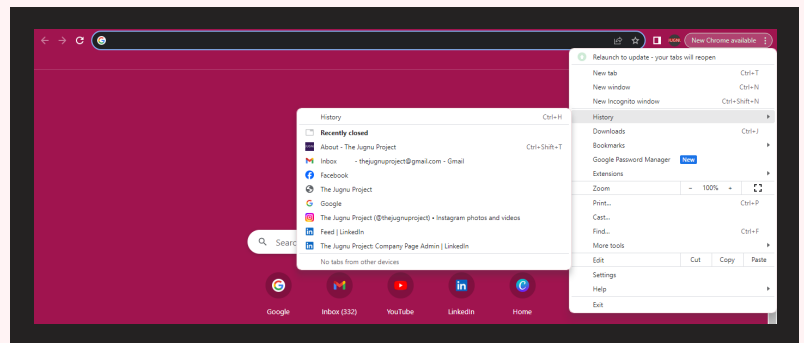
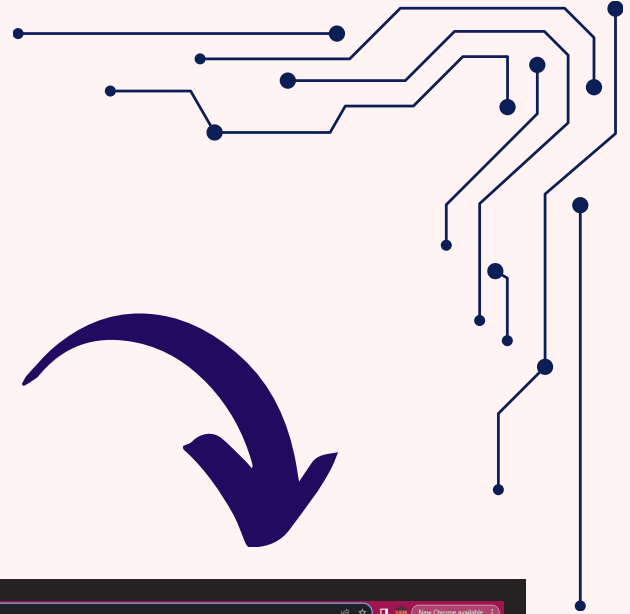
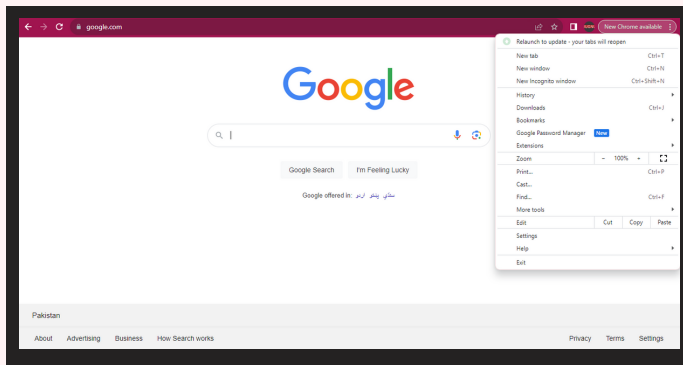
**1.5** On the top left, choose the “*Clear Browsing History*” option. A pop-up will open, showing you the different types of history that you can clear / delete.

**1.6** It will also include a duration of time for which you can clear history - be it the last hour, the previous 24 hours, the previous week or months. Select whatever option you find safest.

**1.7** If you want to remove certain items from your browser’s history, only select the boxes next to those items.

**1.8** At the top right, click *Clear Data*. Your chosen history will be removed.





2. When using your **android phone**, you can clear your browser history by taking the following steps:

**2.1** On your android phone, open the Chrome application / browser.

**2.2** At the top right, click *more* (or click on the three (3) vertical dots).

**2.3** If your address bar is on the bottom, swipe upwards on the address bar. Tap *History*.

**2.4** If you want to view / visit a particular site, tap on the particular entry that you wish to delete.

**2.5** To open the site in a new tab, touch and hold the particular entry. At the top right, click on *more* (or click on the three (3) vertical dots). Select *Open in a New Tab*.

**2.6** To copy a site, touch and hold the particular entry. At the top right, click on *more* (or click on the three (3) vertical dots). Select *Copy Link*. Additionally, a small pop up might also appear on your screen saying *Copy* - tap on that to copy the link.

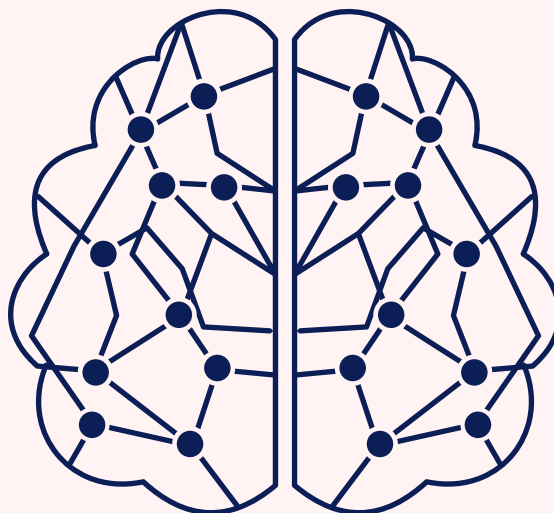
**2.7** Tap *Clear Browsing Data*.

**2.8** Next to Time Range, select the duration of your browser history you wish to delete.

**2.9** Be sure to uncheck / unselect any data that you do not wish to delete from your phone.

**2.10** Tap *Clear Data* to remove unwanted data.

**2.11** You can also tap on the small numbered window in Google Chrome, to close any additional / unnecessary tabs.



3. When using your **iPhone or iPad**, you can clear your browser history by taking the following steps:

**3.1** On your iPhone or iPad, open the Chrome application / browser.

**3.2** At the top right, click *more* (or click on the three (3) vertical dots). Tap *History*.

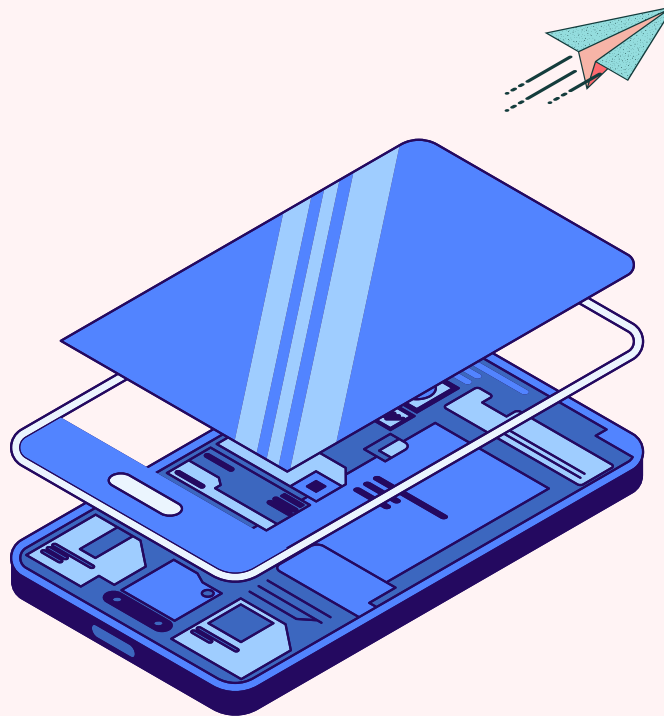
**3.3** At the bottom, tap *Clear Browsing Data*.

**3.4** Be sure to click on the checkbox next to *Clear Browsing History*. It may already have been checked by default.

**3.5** Uncheck any items that you do not want to delete.

**3.6** Tap *Clear Browsing Data* (it will pop up again, as confirmation).

**3.7** At the top right, click on *Done*.

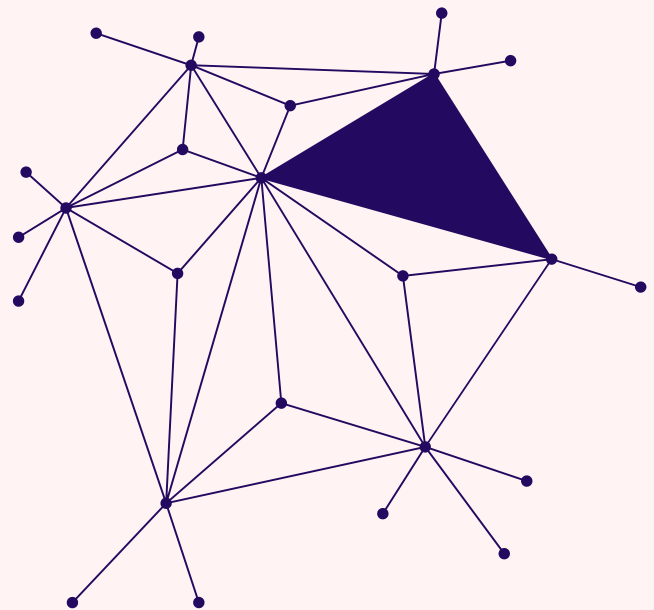




### **Create a Safe Email Account.**

It may be best to create a separate email account that only you know about; especially if your abuser tracks your online activity and has access to your passwords and other login information. You can create a generic email, without including your real / full name in the email itself. You can then use this email safety planning and other important communication(s), such as applying for jobs and even asking for help from family, friends and / or service providers; without raising any suspicions.

In order to continue keeping up appearances, always keep your monitored account(s) active with non-critical emails and communication. This way your abuser(s) will remain unaware of your actions, as you carefully plan your escape. Use several different methods of communication, so that you will know if anyone tries to contact you elsewhere. Additionally, certain encrypted email services may even provide an added layer of security.



## Adjust Your Social Media Settings for Increased Safety.

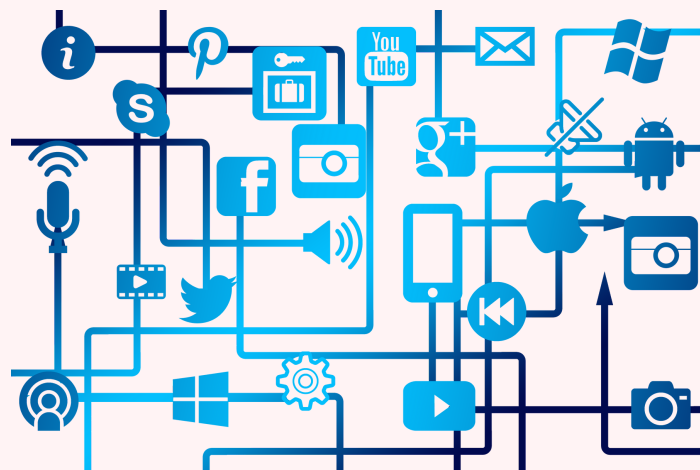
While content creation and sharing on social media has allowed many people to earn a living doing what they love, it has already created security risks for others. Staying on top of your social media account settings can drastically help to reduce some of those risks to safety and privacy.

By switching your account to Private Mode, you deny other users (except a chosen few) access to your profile information. You can also choose which person(s) can view how much of your profile page(s). Without your permission, no one can see your online activity. Almost all social media platforms allow you to block users, as well; which can help you protect yourself online from people you do not wish to interact with. However, before blocking an individual, consider how this may impact your ability to document their abusive behavior; especially if it is escalating. Once you have blocked someone, you will no longer be able to see any messages or comments that they are sending your way.

Additionally, try to refrain from posting on your social media account(s) in real time. Do not post anything that might give away your current location to your followers. For example, if you have gone to a restaurant to eat, wait until you are home (or the next day) before you post anything online about the excursion. These are small but effective steps to ensure that unwanted people do not follow you or show up at your location unannounced and / or uninvited.

Be careful not to tag any specific locations (such as the neighborhood grocery store, or your favorite restaurants, etc.) in your social media posts, as this might give people trying to locate you clues about your whereabouts.

Remember, you can always set firm boundaries for your protection and safety, and that of your children. Ask your social group(s) and your friends, family and / or acquaintances not to post any personal information, photos or check-ins that you are not comfortable with. Teach your children to do the same, if you feel this could help keep you all protected from abuse. Check your social media profiles to ensure that your privacy settings are strict. You can also disable the ability for others to tag you in their (or other) photos and posts. Similarly, do not post anything regarding other people without their consent - you may be jeopardizing their safety, as well as your own.







## **Protect Your Devices On The Go**

Our phones - and sometimes even our laptops - accompany us wherever we go. Sometimes we use our own data plan, but at others we may need to use a public WiFi. It is important to understand how vulnerable our phones and other devices can become when connected to a public WiFi network.

If you can afford to invest in a good VPN, your IP address / location can be easily masked; also helping to keep your web browsing hidden. This is especially useful if you are using a public network - or if you are browsing at home, out of sight of your abuser(s).

If you cannot currently invest in a paid VPN, there are some free VPN services available - but be careful when choosing one of these. You can also make sure that you only browse secure sites (that use https://) - protocol that can help exponentially increase your security online. While someone may still be able to see that you are on a specific site, they will not be able to see what you are doing, or looking for, on that site.

## **Cell Phone Safety**

Cell phones have become increasingly embedded in peoples' daily lives; to the point that they can provide others instant updates about your whereabouts and activities. They can be used to track your location, and even retrieve your call, text and browsing history.

If you are living with your abuser, you may want to use a separate phone device entirely (such as a temporary or burner phone) when planning your escape. You could even keep it in a safe place and keep it switched off except at certain times during the day (or night) when it is safe to switch it on and communicate with the outside world. Always be sure to erase all phone activity after each usage, if your device(s) is being monitored. You may even save critical numbers under pseudonyms to ensure anonymity and security.

If you are concerned that your partner may be secretly monitoring your phone, you could take it to the nearest cell phone service center to check for any spyware that may have been downloaded, unbeknownst to you.

If you use Apple products, you can learn about Safety Check. This is an important tool that allows users to quickly view and reset information sharing and access with people, apps and devices.



### **Enable Additional Authentication**

When logging onto online accounts, whether on your phone or devices, there is usually a prompt for further authentication. This is known as two-factor authentication. It allows the user to add an extra layer of protection on their account by sending a special code to their chosen device every time a login occurs. This means that if someone is trying to log into your account without your permission, you will promptly be informed of it and can take measures to prevent them from accessing your account(s).

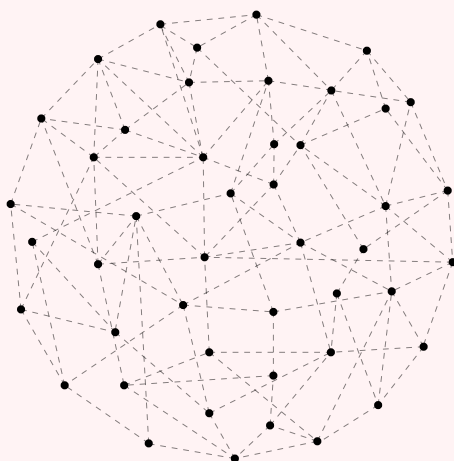
You can take these steps to protect your email accounts and social media profiles; effectively preventing others from accessing your personal and / or financial information.

### **Secure Your Home Network**

A secure network connection starts with the router. The router communicates between the internet and all the devices in your home in order to deliver a WiFi connection. When installing a network connection, there are several things to be mindful of. Structures such as a fireplace or thick walls can block router signals or intercept the internet connection. Be sure that you are purchasing a router which is the correct size for your home and consider the amount of devices that will be connecting to it.

Additionally, be aware of how secure your router is. Routers that are not secure are vulnerable to being hacked - which can allow someone to potentially install malware onto one of your devices. Try to find a router that has network level protection, including automatic updates, signed firmware updates and device quarantine.

Finally, the router you use should be easy to navigate and control. You can ascertain the different features that might be suitable to the different members of your household that would be using the network and WiFi connection. This includes parental controls, guest networks and network management. Do not skimp on your router, as it is an essential ingredient towards keeping a secure home network.





THE JUGNU PROJECT

*Pakistan's Digital Domestic Violence Resource Centre*

<https://thejugnuproject.com/>