# Table of Contents

- Hello. ........................................... 1.1  
- How are you being tracked? .................1.2  
- Risks ............................................. 1.3  
- Set a killer password .......................... 1.4  
- Protect your browser .......................... 1.5  
- Social Media & Devices ........................ 1.6  
- Final words & thank yous .................... 1.7
“No matter what I did - he found me. Now I know how he did that...”

“Wow, yes it really is an eye-opener!”

“This is the first time anyone's been able to shed any light at all on this - usual authorities seem to be clueless...”

**WHO IS THIS GUIDE FOR?**

Everyone, everywhere. Though written with women dealing with domestic abuse or stalking in mind, the guide and its principles can be used irrespective of gender, location or situation.

Does someone have pictures of you and you don’t know how or why? Do they keep showing up unexpectedly to places where you are? Do they know things about your life that you haven’t told many people? Then you may be being stalked.

**WHAT IS THIS GUIDE ABOUT?**

Modern technology such as the internet/mobile phones etc., has made it increasingly easy for abusive partners to stalk, intimidate and threaten their targets both online and offline. The good news: you can take measures to protect yourself!

Assess your risk and take back control with this guide of best practices.

**HOW TO USE THIS GUIDE**

There are many ways someone can track you down. The chance and ease of this happening will depend heavily on your personal circumstances and that of your abuser. This guide is not the complete answer. This guide doesn’t include all of the ways abusers can track someone, but it is a collection of tips and support including our best finds. Off you go!
Hello.
How are you being tracked?

Following your online habits

While surfing the web, sophisticated technology is collecting data on you through email providers, mobile-phone apps, search engines, browsers, social-media messengers. In the hands of your abuser, this information could endanger your personal privacy, your control over your identity online and your access to free information.

The information that can be collected can be information you provide yourself when you register/create an online account such as physical address, email, personal interests and details as well as information you do not provide knowingly (for example: data from your smartphone like wifi-signals or GPS locations of the places you visited, websites your surfed in your browser).

Emails and pictures can also track you by transmitting data like location, time, sender and receiver

“Social websites like facebook are by nature a vulnerability for your privacy as your contacts’ timeline can give out information that can be used to track you.”

To assess how secure your online presence is, please also consider how your children’s and friends’ online presences and their connections with you can affect your own security. If you or your relatives have received a direct threat online by email, direct messaging or other online means, please contact the police and supply evidence.

Even though you realise that you unknowingly divulged information, you can now act.

Tips to mitigate vulnerability:

- Log out of social media sites after your visit (trackers usually won’t find you when you’re logged out neither would your contacts)
- Install browser extensions that block trackers and ensure better privacy
- Be mindful when posting on social media
- Prefer anonymous chat and erase chat history

Keep in mind your stalker can potentially monitor the devices of anyone they’ve come in contact with, including your children or anyone that has stayed in the same house. At the end, your own security also depends on your friends and family

DIY Online Security by CHAYN is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.
Analyzing your risks

1. Identify your security risks

You should take as much care to protect your online presence as you do with your physical one. Securing your online presence is crucial to health and happiness; if someone intrudes upon our online space, it is easy to feel violated.

2. Assess the strength of your security practices

Ask yourself:

**WHO?** is your stalker/abuser? Do you know the abuser? Is the abuser connected to you? Are they financially resourceful? Politically/socially influential? Do they know how to use technology?

**WHERE?** Does your environment increase the threat? What are the laws and policies enforced? What are the cultural norms of your abuser’s community, family or your own?

If you don’t know, try talking to people you trust to get information from them. If it is difficult to obtain information about safety and privacy laws, it is likely that they are either non-existent or weakly enforced, so your environment increases the threat.

**HOW?** Is it easy to bribe someone where you live? Can your abuser use their economic/social influence to access your information? Does your abuser have power over your relatives?

3. Security areas to prioritise

Take the Privacy Test by Smart Privacy.

Only YOU know what devices you use, what apps and services you access, how you use them and what you use them for. Take that context into account to decide what strategy to use and remember that it may require a change in behaviour or some level of inconvenience, so choose the strategy and recommendations that best suit your situation.

**Devices and apps**

Select carefully what device, app or network you trust with your information. Remember your mobile phone and laptop are likely to be collecting your data, which could be shared with service providers or could be maliciously accessed by a hacker.

Your connections, applications and services may be insecure, may have been compromised, could be used to monitor your activity.

**Email account**

It is at the centre of everything you do online, such as other accounts you create on other websites, social-media platforms, etc… If your email is compromised, it puts at risk all of your other accounts and data.

**Spyware**

Your phone can be set to record and transmit any sounds within the range of its microphone without your knowledge. Some phones can be switched on remotely and brought into action in this way, even when they look as though they are switched off.

---

DIY Online Security by CHAYN is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.
Easy steps to fight the most common vulnerability

**HOW TO CREATE A STRONG PASSWORD**

1. **Password protection**
   - Visit [How Secure Is My Password](#) to test the strength of your passwords
   - Never recycle or reuse passwords
   - Do not use the same password across multiple sites - Create a new or different password for every site you sign up to
   - Do not let your browser save your passwords
   - Think passphrase instead of password
   - Use upper or lower case letters, numbers, symbols - See [Strong Password Generator](#). Password Managers usually have a built-in password generator to create complex passwords

2. **Use a password manager**

   Password Management software stores encrypted versions of your passwords so you can use a unique, secure password for every service without having to remember every password. There are plenty of [free Password Managers](#) to select from, for example, KeePass (see [how to setup and use it](#), LastPass and Padlock.

3. **How should you change your password?**

   There have been debates about how often we should be changing our passwords. It is also recommended that we change your passwords every 3 – 9 months. We recommend that you change your passwords as often as you need in order to feel secure.

4. **Two-Factor Authentication (2FA)**

   Two-Factor Authentication (2FA) makes it harder for anyone attempting to hack your accounts. Instead of signing into your accounts using one step (your password), you enter a second piece of data, a short code sent to you in an email, or text, or generated by an app on your phone. See which sites allow you to enable two-factor authentication [here](#).
Set a killer password
How to protect your browser

First, test how safe your current browser is with Panopticlick

Browser Privacy Settings - Do Not Track and Private Browsing Windows

DO NOT TRACK

Chrome > Settings > Show Advanced Settings > > Privacy > Send “Do Not Track” request with your browser traffic
Firefox > Options > Privacy > manage your Do Not Track settings
Safari > Menu > Preferences > Privacy > Website tracking > Ask websites not to track me

Explorer > Tools (Alt + X) > Safety > Turn on tracking protection > Enable
Alternative Browsers and Search Engines

- **Brave** is a browser which automatically blocks ads and trackers
- **Tor** is a browsing software that enables you to surf the web anonymously
- **DuckDuckGo** is a private search engine that does not track its users
- **StartPage** is a private search engine that does not record your IP address or track your searches

**Incognito Mode (Chrome)**

- Incognito mode on the web prevents Google Chrome from saving a record of what you visit and download.
- Customise and control Google Chrome > New incognito window
- Or hold down: Ctrl + Shift + N

**New Private Window (Firefox)**

- New Private Window opens a private browsing window in Firefox.
- Open menu > New Private Window
- Or hold down: Ctrl + Shift + P

**New Private Window (Safari)**

- New Private Window stops Safari from keeping track of what web pages you're viewing.
- File menu > New Private Window
- Or hold down: Command + Shift + N

**InPrivate**

- InPrivate helps prevent Internet Explorer from storing data about your browsing session.
- Tools > Safety > InPrivate Browsing
- Or hold down: Ctrl + Shift + P

**Use a VPN**

- A VPN, or a Virtual Private Network, is a way of disguising your IP and encrypting all of your internet traffic so that no one can find out what you’re viewing online.
- Free VPN: OkayFreedom (please note: the free version of OkayFreedom is ad-supported) TunnelBear
**Tor**

The Tor Browser is designed to help keep you anonymous and is a simple yet effective way of browsing the internet without revealing your identity to anyone.

Download it [here](#).

---

**Browser Extensions**

Browser extensions (Add-ons/Plug ins), are programs which extend or customise a web browser. Extensions can be used to protect your privacy by blocking third parties from tracking your online activity. **WARNING:** Extensions can also be malicious [examples](#).

**Recommended extensions:**

- [HTTPS Everywhere](#) (Hypertext Transfer Protocol with Secure Sockets Layer)
- secures and encrypts your internet traffic
- [Privacy Badger](#) blocks tracking [cookies](#)
- uBlock Origin is an adblocker

**Erasing your browsing history**

- [Chrome](#) > History > Clear browsing data
- [Firefox](#) > Options > Privacy > History
- Recommended PC Cleaners:
  - CCleaner
Protect your browser

- BleachBit

DIY Online Security by CHAYN is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.
Social Media & Devices

Facebook

Who Can See My Stuff?
Who Can Contact Me?
How Do I Stop Someone From Bothering Me?
Twitter

Security and Privacy
Security and privacy
Change your security and privacy settings.

Security

Login verification
☐ Verify login requests
After you log in, Twitter will send a SMS message with a code that you'll need to access your account.

Password reset
☐ Require personal information to reset my password
When you check this box, you will be required to verify additional information before you can request a password reset with just your @username. If you have a phone number on your account, you will be asked to verify that phone number before you can request a password reset with just your email address.

Log in with code
☐ Allow my account to log in with either a password or login code
You will be able to log in with your password, or by requesting a secure login code. Learn more
☐ Always require a password to log in to my account
You will be asked for your password every time you log in. This means you will not be able to log in by simply receiving a login code (via SMS or email). Learn more

Privacy

Photo tagging
☐ Allow anyone to tag me in photos
☐ Only allow people I follow to tag me in photos
☐ Do not allow anyone to tag me in photos

Tweet privacy
☐ Protect my Tweets
If selected, only those you approve will receive your Tweets. Your future Tweets will not be available publicly. Tweets posted previously may still be publicly visible in some places. Learn more.

Tweet location
☐ Add a location to my Tweets
When you tweet with a location, Twitter stores that location. You can switch location on/off before each Tweet. Learn more

Delete location information
Deleting location labels from your past Tweets... This may take up to 30

Devices

Disable Location
How to secure your Android phone: Switch off Wireless and GPS location (under Location Services) and mobile data (this can be found under Settings > Personal > Location). Note: Only turn on location settings as you need them. It is important to have these services turned off by default as this will reduce the risk of location tracking, save battery power and reduce unwanted data streams initiated by applications running in the background or remotely by your mobile carrier. (Taken from: https://securityinabox.org/en/guide/basic-setup/android)

See Turn Off Location Services through Settings

How to secure your iPhone: Switch off Wireless and GPS location: Settings > Privacy > Location Services and either turn off all Location Services using the Location Services slider or use the individual sliders for each location-aware app or item on your device. To disable Location Services for all websites, turn off Location Services for the Safari app. See How to Turn Off Location Services on iOS]

Messaging Apps

Whatsapp

WhatsApp messages are encrypted (meaning the content of the messages you send can only be seen by you and the recipient) but metadata about who you chat with and for how long is collected and stored.

Signal

Signal by Open Whisper Systems is a free and open-source encrypted voice calling and instant messaging application for Android, iOS and desktop. It uses end-to-end encryption to secure all communications to other Signal users. Signal can be used to send and receive encrypted instant messages, group messages, attachments and media messages.

Security Tips Every Signal User Should Know

Additional Advice

- IMPORTANT: Take the Privacy Test by Smart Privacy
- Create a Google Alert for your name

DIY Online Security by CHAYN is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.
Do whatever you feel you need to in order to feel and stay safe.

We hope you enjoyed our guide and found it useful!

To read the full, Advanced guide in English click here.

Thank Yous!

This guide is a project by CHAYN, an open-source project that uses technology to empower women against violence and oppression so they can live happier and healthier lives. CHAYN created a set of privacy guides after several interactions with real-life domestic abuse survivors, reading scores of articles on doxxing of women online, and from our very own experiences as women who use the internet. Technology and the internet opens us up to new worlds and provides us information at the touch of a button, but it can also open us up to security risks.

This guide focuses on online stalking, and was created with the help of survivors of domestic violence in many countries. We aim to provide the necessary tools and knowledge to minimise the chance of being tracked by the abusive person(s) after having left the abusive environment. However, the guide can be useful to anyone who is being stalked or tracked online by an abuser, regardless of their gender, location or situation. CHAYN believes in survivor-led design, which means not only do we listen to survivors, they’re part of the production team - they volunteer with us.

Using existing online privacy guides tailored for women as inspiration and for reference, CHAYN volunteers began building this guide by crowdsourcing content. There was a lot to cover but we were determined to build an exhaustive easy-to-understand guide that could benefit all internet users. After we had a Version 1 ready, we sent it out to security experts as well as survivors of domestic violence, and people who have experienced stalking and other forms of cyber harassment to give us their feedback. We then assessed their comments and added information to the guide, making it as inclusive as possible.

Then we introduced Securikitty (meoow!) to help make the guide more user friendly, approachable and to help remind readers when to take breaks and encouraging them to stay strong through the process of protecting themselves.

If you found this guide useful, you may be interested in some of our other resources that we have produced such as How To Build Your Own Domestic Violence Case Without A Lawyer and information about domestic abuse in Pakistan, India and Italy Some of these will only be in English but we’re working on more translations.

The content for this document is openly licensed using the Creative Commons Attribution-ShareAlike 4.0 International. All are invited to remix and distribute it as long as it is appropriately attributed.

We would like to thank our amazing partners and allies who have helped us by giving feedback and adding. We would like to thank all the CHAYN volunteers who helped put this guide together from different parts of the globe especially Nikki, Sam, Lee, Dina, Reema, Clarice, Sarah and Aliya. We would also like to thank the many NGO’s and security geeks who helped shape this guide; Sara Baker of Take Back the Tech!, Nighat Dad, Hamara Internet, Soraya Chemaly, Randi Lee Harper, Jacquie Vernimont, Martin Shelton, Right2Know, Lawyers Against Abuse (LAA) and folks at Tactical Tech and Engine Room. We would also like to say that this guide was built by consulting many resources, such as the DIY Feminist Security Toolkit, NNEDV’s TechSafety, Feminist Frequency, The Smart Girl’s Guide to Privacy: Practical Tips for Staying Safe Online, and Tactical Tech’s various resources.

A special thank you also to all the translators who helped us translate the guide into the different languages: Naveedullah Pasoon (Pashto), Muhibullah Shadan (Farsi), Mahmoud Qudaih (Arabic), Aisara Yessenova (Russian), Sandra Hernandez Garrido (Spanish), Mariam Faisal (Urdu) and Haude Le Guen (French).

Our projects are always a work in progress and we want your help in making our projects better! If you have any suggestion or ideas, please email us at team@chayn.co.

Thank you so much for collaborating with us. This will make a real difference to thousands of women who might be feeling alone and powerless. We want to make sure they know, they’re not. We’re here and so are many others.

The CHAYN Team.
Time for a quick cat nap