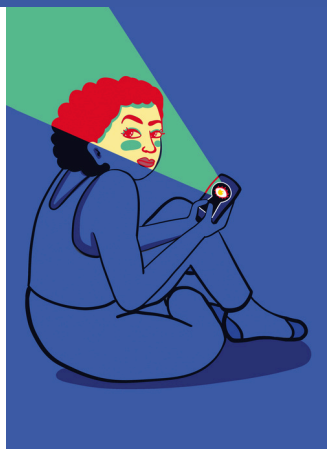
“University girls… are now scared to join WhatsApp study groups because they get stalked.”



#HeyFriend, have you faced unwanted, insistent attention on the internet?

Have you thought twice about going somewhere, or commenting on a post, just because a person might use it to harass you?

Are your posts being monitored and shared with people (family, colleagues, peers) without your consent?

You’re not alone.

This is stalking on the internet. You may keep blocking accounts, but somehow they always (or mostly) seem to know what you are up to.

How does it happen? How can you protect yourself?

The first thing to know is, sometimes you really don’t need a special application. Your own phone and accounts have enough data, if unprotected, to arm your stalker with relevant information.

But let’s talk about prevention first:

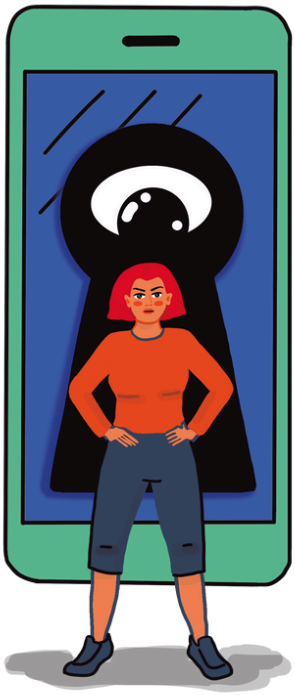
- **Be cautious about app downloads:** Only install apps from trusted sources.
- **Keep software updated:** Regularly update your operating system, apps and security software.
- **Be mindful of public Wi-Fi:** Avoid accessing sensitive information on unsecured networks.

Now, in a situation where you absolutely have to be in touch with someone you know or suspect to be your stalker (in co-parenting or co-working situations), here are some first steps — **that we hope you don’t have to use for long:**

- **“Restrict”, “mute” or “hide”** the stalker’s profile and updates on social media.
- **Store all unwanted** textual (SMS, emails, DMs) communication from the stalker as evidence of stalking and abuse.
- **Engage only when you feel like it.** Set up filters in your email and messaging apps to sort or redirect messages from the stalker.
- For email, **create a new folder** in your email account specifically for the stalker's emails. For each email address used by the stalker, create a filter that automatically directs their emails to the designated folder.
- If the stalker contacts you from a new email address every time, **set up additional filters** for commonly used keywords or phrases in their emails.

Next, how can you protect your existing accounts to avoid data leaking into the hands of your stalkers?

- **View the pin location** of your home, workplace or other places you commonly visit on Google Maps and other mapping services to look for any content that violates your privacy.
- You might also find **defamatory content** about these places. If you find private or false information, report it to the platform immediately for removal.
- Some shared accounts such as Netflix or gym memberships also include **location features.** Check if location is activated in any apps or if there are any linked devices as a quick safety step.
- If you find that your private information has appeared on public records maintained by either a government agency or a privately-owned online database, contact the website/ service and **ask them to remove your private information** or your entire profile.
- **Disable your notification history or turn off notifications** from some contacts (messages and emails) that you need to keep private — if you suspect that your stalker has physical or remote access to your device.



Additional tip:

Fake social media profiles (of you) may be created to manipulate you and your social circle. Monitor and protect your online presence by creating a set of Google Alerts to receive email notifications for:

- Your full name (with variations in spelling, and past names, if any).
- Your phone number, email address, street address, etc.
- Use quotation marks for exact phrase matching.

For more information about email and chat filters, blurring your home location on Google maps, and managing notifications, scan: