Let's talk about

STALKING

AND EX-LOVERS

(and situationships too)

What is STALKING?

Sometimes, the digital world may not be as friendly as we had hoped. In it, we may be surrounded by violence, discrimination, exploitation, abuse, harassment, and stalking — similar to our offline world.

If you're feeling uncomfortable or as though your activities are being monitored and watched, **we need to talk about stalking.**

Do you feel like someone is following you online, even though you may have blocked their profiles?

There are so many options online — applications, social networks, chatting platforms and even bank accounts — which may be used to manipulate you and keep track of your digital activities without your consent.

A stalker's tools and methods are constantly evolving, so stay up to date — periodically compare and review resources available to you.

#StalkerAlert

Did you know that certain applications, when they have access to your phone, can create havoc beyond your imagination?

These applications may have been installed by your stalker (ex-partner or family or people with access to your devices) or by yourself, under the guise of being a different application or help!

Do you know what these spy programs, **also called stalkerware,** can do on your devices?

- View call history, text messages (even deleted ones) and record phone calls.
- Take screenshots and record video from your screen.
- Activate camera and microphone to capture photos, videos and audio of what is going on around you.
- GPS location tracking and location history viewing.
- Read messages in instant messaging and social networking applications.
- View browsing history.
- Access photos, videos, documents, calendars and other files.

CAN YOU PREVENT STALKING?

It's hard when a relationship ends, although it can also be a relief! Whatever your case, it's important to protect yourself in every way — including digitally. Check who can access your devices to prevent misuse or accidental exposure of your personal information!

Here are some good practices regardless of your relationship status:

Avoid leaving devices unattended, especially in situations of conflict or relationship breakdown.

Establish clear privacy, intimacy and security agreements. If possible, avoid sharing access to devices and accounts.

Install only apps from trusted sources and know what actions they perform.

Regularly update the operating system, applications and security software of your devices.

Be careful with public Wi-Fi connections: avoid accessing confidential information on unsecured networks.

Any break up is complicated, so make space to take care of yourself – and your tech!

- Be aware that some shared accounts, such as Netflix or a gym membership, also include location features.
- Take a moment to check if location permissions are enabled in any application, and review who has access to it.
- Check linked devices on your accounts as a quick security measure... Your once-shared Spotify or YouTube account may leak sensitive information you don't want in someone else's hands.

DATING APPS: YES TO CONNECTION, NO TO STALKERS!

Hmm.. it's been a while since your breakup and maybe you're ready to dip your toes into the dating pool again. Maybe you want to try out a dating app — but if you're being stalked, this may incite your stalker. It's important to be aware of geolocation and other features in the dating app you choose.

Some dating apps allow you to preemptively block other users through their phone numbers. However, location-based apps also offer a feature that allows users to share profiles they like with their friends. For example, Bumble's "Refer a Friend" feature creates a link to the profile that can be shared. A friend of a stalker in your area (dating apps show profiles within a radius or region) could stumble upon your profile and share their information via screenshots or the shareable link. Accessing and viewing a profile through such a link does not mean the app will alert you to profile interaction.

Some dating apps allow stalkers to access the almost exact location of users: in Bumble and Hinge, the accuracy is 2 meters radius; in Grinder, 111 meters. Even if the stalker is blocked from the app, they can create multiple accounts with different cell phone numbers to access profile information.

ARE YOU BEING STALKED BY YOUR PARTNER OR EX-PARTNER?

A break up is not easy. It often involves complex and painful conversations — anger and arguments. If you were in a toxic or difficult relationship, you may have witnessed violence too. It's hard to think about your tech at these times. At Take Back The Tech! we developed a flowchart that can help you determine if someone could have tampered with your phone.

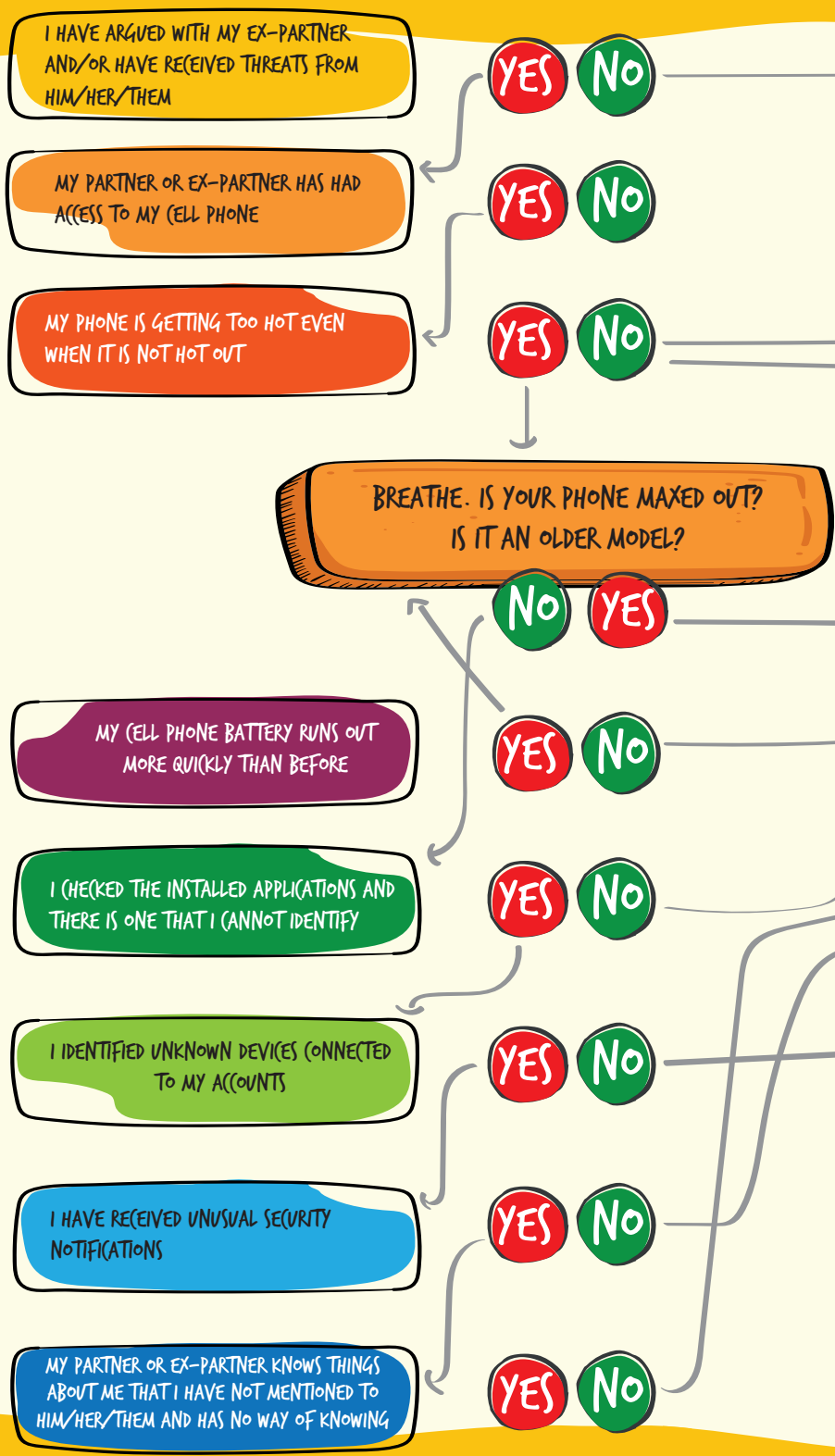
You can find more tools to help you assess risk at Take Back the Tech!

NOTE: These are just a few recommendations. If you detect any malicious behavior, seek help from feminist organisations and allies or your local women's shelter. For digital safety support:

Feminist Helplines Index:
https://feministhelplines.org/
InterSecLab.org for support in Latin America

Whatever your situation, we have your back.

Contact us:
help@takebackthetech.net
@takebackthetech
on x.com


I HAVE ARGUED WITH MY EX-PARTNER AND/OR HAVE RECEIVED THREATS FROM HIM/HER/THEM
YES
NO
MY PARTNER OR EX-PARTNER HAS HAD ACCESS TO MY CELL PHONE
YES
NO
MY PHONE IS GETTING TOO HOT EVEN WHEN IT IS NOT HOT OUT
YES
NO
BREATHE. IS YOUR PHONE MAXED OUT? IS IT AN OLDER MODEL?
NO
YES
MY CELL PHONE BATTERY RUNS OUT MORE QUICKLY THAN BEFORE
YES
NO
I CHECKED THE INSTALLED APPLICATIONS AND THERE IS ONE THAT I CANNOT IDENTIFY
YES
NO
I IDENTIFIED UNKNOWN DEVICES CONNECTED TO MY ACCOUNTS
YES
NO
I HAVE RECEIVED UNUSUAL SECURITY NOTIFICATIONS
YES
NO
MY PARTNER OR EX-PARTNER KNOWS THINGS ABOUT ME THAT I HAVE NOT MENTIONED TO HIM/HER/THEM AND HAS NO WAY OF KNOWING
YES
NO

THE PROBABILITY IS LOW, STILL KEEP AN EYE OUT FOR ANY CHANGES

IT IS POSSIBLE THAT YOUR PHONE HAS BEEN TAMPERED WITH. DON'T BE ALARMED, FIRST CHECK THE APPS AND PERMISSIONS.

IT IS VERY LIKELY THAT YOUR PHONE HAS BEEN INTERVENED. CONTACT ORGANISATIONS THAT CAN HELP YOU.

SOME RECOMMENDATIONS:

- TAKE A DEEP BREATH BEFORE TAKING ACTION. IF SOMEONE CAN ACCOMPANY YOU, ALL THE BETTER.
- DOCUMENT ANY STRANGE BEHAVIOR OR APPS.
- INVESTIGATE APPS YOU DON'T RECOGNISE.
- PUT A PASSWORD ON YOUR PHONE.
- CHECK THE PERMISSIONS YOUR APPS HAVE.
- CHECK FOR ANYONE ELSE'S ACCOUNTS OR DEVICES LINKED TO YOUR APPS.
- KEEP IN MIND YOUR LOCATION MAY BE UNDER OBSERVATION. IF YOU ARE ON THE MOVE, CONSIDER LEAVING YOUR PHONE BEHIND.

SUSPECT YOU'RE BEING STALKED?

TAKE ACTION!

Remember that if you are being monitored, your attacker may be aware of any changes you make on your devices and this could upset them even more. If you suspect your device is compromised, document, analyse and seek support rather than making changes on your devices.

If you seek help, try to use a separate device to reach out.

takebackthetech

takebackthetech.net/stalking

APC
ASSOCIATION FOR PROGRESSIVE COMMUNICATIONS

Source: Take Back the Tech! Feminist Learning Circles with Marla from InterSecLab and Rohini Lakshané