DeStalk TOOLKIT

for providers working with victims/survivors

Supported by the Rights, Equality and Citizenship Programme of the European Union (2014–2020)

DeStalk Toolkit for providers working with victims/survivors

Contents

UNA CASA PER L'UOMO
società cooperativa sociale

DeStalk: detect and stop stalkerware and cyberviolence against women
Una Casa per l'Uomo
Elena Gajotto – Chiara Moretti – Luisa Casagrande
January 2022
Rev. October 2022

Glossary of cyber violence terms

Despite technology having being a fundamental part of our every day life for a long time, cyberviolence has only recently come to the attention of professionals and policy makers. A first EU-level definition of cyberviolence was given by GREVIO in November 2021

> The **digital dimension of violence against women** encompasses a wide range of acts online or through technology that are part of the continuum of violence that women and girls experience for reasons related to their gender, including in the domestic sphere, in that it is a legitimate and equally harmful manifestation of the gender-based violence experienced by women and girls offline.
>
> GREVIO General Recommendation No. 1 on the digital dimension of violence against women

According to this definition, cyber violence is called the digital dimension of violence against women and encompasses abuses perpetrated online or through digital devices.

It is important to understand that the following list with forms of cyber violence is not exhaustive because forms of cyberviolence change and develop following the constant and rapid evolving of digital technologies. Also, a form of cyber violence may vary a bit in their appearance so that characteristics may overlap. In addition, it happens that the same form of violence may have a different name. As EIGE (2017) pointed out, it would be helpful to have definitions politically agreed as this would facilitate better coordination at inter-organisational level. When cooperating, victim support organizations, perpetrator programmes and law enforcement may overcome as a first hurdle the need to agree on the same definition.

Cyber violence is an umbrella term. That includes all the forms of violence that are perpetrated through ICT. The most common forms are cyberstalking, cyberbullying, harassment and non-consensual sharing of images. As gravy oh. Affirms. In its recommendation., facilitated forms of violence Against women and girls are amplified and facilitated by technology, and this brought to a never seen before escalation of the phenomenon. Violence perpetrated online or through ICT is a continuum of offline forms of violence, and it is not a phenomenon separated from offline violence., because often. It follows the same patterns of offline violence, and it leads to psychological, social and economical consequences for women and girls and can transform into physical, sexual or psychological.

As specified by EIGE[1] Cyber violence against women and girls includes a range of different forms of violence perpetrated by ICT means on the grounds of gender or a combination of gender and other factors (e.g. race, age, disability, sexuality, profession or personal beliefs).

All acts of cyberviolence can:

a. start online and continue offline such as in the workplace, at school or at home;
b. start offline and continue online across different platforms such as social media, emails or instant messaging apps;
c. be perpetrated by a person or group of people who are anonymous and/or unknown to the victim;
d. be perpetrated by a person or group of people who are known to the victim such as an (ex) intimate partner, a school mate or co-worker

Due to the many possibilities offered by ICT, there is a wide variety of forms to carry out gender based cyber violence. The following is a **list with the most relevant methods in which gender based cyber violence is carried out.**

[1] EIGE (2022) *Cyber Violence against Women and Girls Key Terms and Concepts* **Cyber Violence against Women and Girls. Key terms and Concepts (europa.eu)**

Glossary of cyber violence terms

Cyber stalking

involves intentional repeated acts against women.It is committed through the use of ICT means, to harass, intimidate, persecute, spy or establish unwanted communication or contact, engaging in harmful behaviours that make the victim feel threatened, distressed or unsafe in any way (EIGE 2022). Online stalking can be carried out in different ways:

- **Stalkerware** are apps secretly installed on the victim/survivor's device to monitor and track her
- **Hacking or cracking** of communication and data stored online (for example on the cloud) or on private computers that are accessed without consent. This includes webcam hacking which often affects women, and the use of smart home devices to listen to conversations.
- **Cybersurveillance** use of ICT to monitor activities, locations and social interactions of the victim/survivor. This can be done through specific devices (GPS trackers, fitness trackers, etc.) or through the access to online accounts (es. Google or iCloud, etc.)
- **Following** the woman **online**, monitoring her social media accounts, replying to all her posts, joining the same groups, tagging her obsessively. This can also be done with fake accounts

Cyber harassment

is a wider category of threats or other offensive behaviours by an individual or a by a group of persons aimed at offending, disparaging, or belittling a person through digital public and private channels. Online harassment encompasses:

- Non requested emails or messages
- Offensive or inappropriate requests on social media or chats
- Threats of physical or sexual violence through emails, mnessages or chats
- Hate speech, that is the use of offensive, denigratory or threatening language online
- Inappropriate or sexual comments to social media posts or contents

Cyberharassment includes:

- **Slander** refers to damaging someone's reputation by making a false statement about them (e.g. spreading rumours via social media).
- '**Slut-shaming**' is according to CYBERsafe (2020) the online "practice of criticizing people, especially women and girls, who are perceived to violate expectations of behaviour and appearance regarding issues related to sexuality".
- **Online threats** of rape, abuse or death
- **Body shaming**. Messages or comments written with the intent of humiliating someone by making mocking or critical remarks about their body shape or size.
- **Gendertrolling**. Malicious acts online involving the sending or submission of provocative emails or social-media posts, including rape and death threats. Similarly to trolling, also gendertrolling aspires to fment dispute and cultivate a following, inciting an angry or upsetting response from its intended target (EIGE, 2022)
- **Sexual solicitation**. Receiving unwanted requests to talk about sex or do something sexual in a variety of online contexts, like sending sexually explicit images or engaging in technology-mediated sexual interactions. It can lead to receiving abusive misogynist comments, harassment, and threats, particularly if the victim has rejected the requests in some way (EIGE, 2022)

Non-consensual sharing of intimate content

covers a variety of methods that can be explained by sexual images or videos shared or obtained without a person's consent. This category includes

- **Sextortion**. The act of threatening to publish sexual content (images, videos, deepfakes, sexual rumours) to menace, coerce or blackmail someone, either for more sexual content or for money, sometimes both. The perpetrator can be an ex-partner who obtains images or videos during a prior relationship, and aims to publicly shame and humiliate the victim, often in retaliation for ending a relationship (EIGE 2022)

Glossary of cyber violence terms

- **Non consensual sharing of intimate images**. distribution, or threat of distributing through ICT intimate, private and/or manipulated images and/or videos of a woman or girl without her consent. mages/videos can be obtained non-consensually, manipulated non-consensually, or obtained consensually but distributed nonconsensually. This form is generally known as "revenge porn", but this term is not correct, because it generates the idea that the perpetrator is reacting to something bad that the other person did to him, leading to involuntary victim blaming (EIGE 2022)
- **Creepshot voyeurism** (including downblousing and skirting) refers to taking non-consensual pictures or videos of a partner's or other (unknown) women's intimate body parts (e.g. backside, legs, or cleavage). This can be done with hidden cameras, or when the woman doesn't notice (in the shower, while she sleeps, etc.)
- **Deepfake**. Manipulated or synthetic audio or visual media that seem authentic, and which feature people that appear to say or do something they have never said or done, produced using artificial intelligence techniques. Most deepfakes of women and girls depict intimate pictures or sexual activities and are shared on platforms/adult entertainment websites, without consent to their creation and publication
- **Cyberflashing**. Sending unsolicited sexual images, mostly of male genitalia (Dick pics), using dating apps, message apps or texts, or using Airdrop or Bluetooth.

■ Limiting tech access

In a time when many daily activities are carried out through the use of devices and apps, limiting or forbidding the access to technology has a huge impact on the victim/survivor's life and has the aim of controlling or isolating her. For example, limiting a woman's access to health providers apps prevents her from taking care of her health. Similarly, limiting her access to home banking apps prevents her from accessing her finances and be autonomous. Also, restrictions on the use of devices or connections can hinder her from seeking help.

Ways of limiting tech access include:

- Restricting device or account use, limiting functionalities (e.g camera, microphone, etc.) or controlling when it can be used
- Damaging a device or making it unusable
- Preventing connection to internet
- Changing passwords, settings

■ Other forms

Doxing (sometimes also written as doxxing) is the method of sharing recognisable and often private information about a person (name, phone number, e-mail address, home address, etc.) on an online platform without their consent. As information usually allows victims to be physically located, doxing can also be a precursor for violence in the physical world. Doxing is often perpetrated in the context of IPV (EIGE, 2022).

- **Identity theft**. Using someone's personal information in order to pretend to be them and to get money or goods in their name. Many free apps also allow for **spoofing**, that is deliberately falsifying the information transmitted to a phone's caller ID display to disguise caller identity.
- Electronically enabled **trafficking**, especially of women, using technological devices and social media, often leading to prostitution.

Cyber violence and stalkerware: what to do guide for professionals working with victims/survivors

Cyber violence is a generic umbrella term that refers to different types and forms of gender-based violence perpetrated online, that can be roughly divided into different groups: cyberstalking (through stalkerware or other ICT means), image-based sex abuse (non-consensual sharing of images, sextortion, etc.), cyber-harassment (cyber-bullying, slander, threats, etc.). Digital violence can be consideres as an online extension of forms of violence normally perpetrated in the physical world (such as cyber harassment or cyber stalking). However, ICT also led to the creation of other forms of violence (such as non-consensual intimate image abuse or doxing) that can amplify the scale of harm compared to violence perpetrated in the physical world.

Digital violence can be perpetrated through different devices (smartphones, PCs, tablets, GPS devices, smart home devices, etc.) and on different online platforms (social media, websites, messaging apps, personal accounts, etc.): all of these devices and platforms are constantly evolving, giving abusers new possibilities of perpetrating new forms of violence. Also, the many different devices and platforms allow for different types of perpetrators, that can be known to the victim/survivor (for example, (ex) partner, school mate, colleague, friend, etc.) or individual or group of people unknown to the victim/survivor.

As we know, online digital spaces and offline physical spaces are strictly interwoven and interconnected, and, ***cyberviolence often reflects (or is a precursor for) forms of abuse and victimisation in the physical world, carried out and/or amplified through digital means*** (EIGE 2022).

For these reasons, professionals working with victim/survivors need to carry out thorough assessment of digital violence, and IT safety elements need to be considered and included when safety planning.

Cyber violence and stalkerware: what to do guide for professionals working with victims/survivors

Assessment and evaluation

Assessment helps us identifying any existing form of digital violence, discussing options with victims/survivors, safety planning and collecting documentation and evidence.

Digital violence can be overwhelming, because it can happen anytime, anywhere and in many different ways. Assessment provides validation that their experience is genuine and harmful, and can give reassurance. When working with victims/survivors, it's important to keep in mind all forms of online violence and to know how to face each of them.

Digital violence assessment framework

In the assessment of digital violence it is important to:

- **Listen to the woman's experience**
  - What happened, and how often?
  - How does the survivor think it happened?
- **Consider information abuse**
  - What information is needed to cause what happened?
  - Where is that information stored? Who can access it, and how?
- **Make a list of devices, accounts** – Keep the types of information abused in mind
- **Assess for access**
  - What can the survivor access, what can the perpetrator access?
  - How could those accounts or devices can be secured?
- **Assess for risk**
  - Think about what can be done safely
- **Plan**
  - What are the survivor's goals?
  - How can she reach them in safety?
  - How can evidence be collected safely?

IT safety plan

IT safety planning is not different from the safety planning normally carried out by support services, it is useful to concentrate on the woman's immediate and long-term needs and goals, and to understand how digital violence is interfering with her life. Tech knowledge is helpful when safety planning, but it is not needed.

A good safety plan should be individualized, survivor-driven, and empowering. It is important to member that "safety" can change quickly. When safety planning, survivors should be given tools and strategies so they can manage their risk and safety, taking back some control.

As mentioned before, immediate and long-term needs and goals of the survivor muste be taken in consideration when safety planning:

- **Accountability and legal questions:**
  - Collecting documents and evidence for court
  - Perpetrators accountability and protection measures
  - Civil remedies: divorce, children custody
- **Increased privacy and tech safety**
  - Establishing a safe connection with the perpetrator
  - Increasing the safety of existing social media profiles
  - Creating new accounts and profiles
- **Stopping violence**
  - Understanding how violence is abused by the perpetrator
  - Finding a way to mitigate the abuse
  - Understanding how tech can be used to reduce o prevent abuse

Cyber violence and stalkerware: what to do guide for professionals working with victims/survivors

The pillars of IT safety planning

One of the most crucial aspects that must be considered is documenting the abuse. The survivors should be informed and guided on how to

- Keep a diary of what is happening
- Take screenshots or pictures
- keep originals (emails, messages, voicemails, or apps)
- Store important documents in safe places or dedicated storing apps

Another important aspect concerns the assessment of access and control of devices and accounts:

- How the survivor communicates
- What devices she has
- How she gets around
- Personally Identifying Information (PII) available online

Elements for risk identification

When assessing possible risk sources, it is important to remember that personal information can be memorized in many different devices, apps and accounts that the abuser may have access to, like for example:

- Social Networks (Facebook, Instagram, Tik Tok, etc.)
- Paypal or other electionic payment systems
- Home banking
- Health apps
- Amazon (Incl. Prime Video)
- Food delivery apps (Foodracer, Glovo, JustEat, Deliveroo, UberEats etc.)
- Spotify
- Streaming apps (Netflix, Discovery+. Disney+, DAZN)
- Workout apps (Garmin, Fitbit, MiFit, Strava, Run Keeper, etc.)
- Travelling (Booking, Trivago, TripAdvisor, etc.)
- Dating apps (Tinder, Bumble, etc.)

The following aspects on connections, information and access need to be considered:

- **Connection**
  - What are devices connected to? (other devices, accounts, apps)
  - How are they connected? (wifi, Bluetooth, wire connection)
  - Who controls the connection?
- **Information**
  - What information is being shared?
  - To whom is this information being shared? (another device, online account, etc.)
  - Does the company have a privacy policy?
  - Can you limit what is shared and to whom?
- **Access**
  - How can the device be accessed? (remote access, physical access)
  - What accounts are associated?
  - Who has access?

To facilitate tech abuse assessment and safety planning, you can use the attached "**DeStalk *Digital violence assessment checklist***", which includes warning signs and red flags to detect possible forms of digital violence, indicatingconnected risks and countermeasures.

Cyber violence and stalkerware: what to do guide for professionals working with victims/survivors

Safety measures

When there is the possibility that the perpetrator is monitoring and tracking the victim/survivor's phone the priority is to develop a clear and thorough **IT safety plan** with the woman. Always remember that **abrupt changes can escalate the perpetrator's abusive behaviour**.

The IT safety plan should tackle the following points:

- **Safe communication channel**
  If the phone is tracked, do not discard it, or delete suspicious apps. Check if the woman can buy a new device, or maybe borrow one: in both cases a new SIM card must be used. Alternatively, check if the woman can use a trusted person's device or a public computer (at the library, for example)
- **Use of the safe device**
  Decide where she should hide it and when/how to use it. The victim/survivor should use the "safe" device for all the conversations that the perpetrator must not know about (e.g., with the support service, lawyer, police, doctor, etc.), but she should still use the tracked phone for other usual activities in order not to raise the suspicion of the perpetrator and to collect evidence. Discuss about the importance of keeping the safe device hidden from her children.
- **Use of online communication and social media accounts**
  If needed, set up safe email and cloud storage accounts, to exchange information with "safe" recipients and store important documents and evidence. Discuss about what kinds of information can be shared on social media.

Another important aspect in safety planning is checking with the survivor for any safety concerns or limitations they may have with turning off their phone. One thing that should be discussed is the potential reaction of the perpetrator if he tries to call and the phone is turned off. Some survivors know they will have to answer for this later and it could escalate risk. Conversations about how long it might take to complete a police report and knowing if the perpetrator always calls at a certain time of the day can be very useful information to help the survivor make informed choices on how and when they can turn off their phone.

Other considerations for planning will be ensuring that the survivor won't need the phone. Do they know exactly where they are going or would they need to use maps? Is there evidence on the phone that they will want to show the police during this discussion? Anything that could lead to them wanting to turn the phone back on. They can then plan for gathering that evidence in a different way so they can show it while still having the phone off.

It's also important to be clear on how fast location can update so people aren't turning on their phones in the parking lot as they leave, but waiting to be a little further away from the station.

Cyber violence and stalkerware: what to do guide for professionals working with victims/survivors

Check the device for stalkerware

If the woman seeking your help has the feeling that her (ex)partner may know too much about her without her sharing information, it will be helpful that you offer the woman assistance to check the device with her.
There are various ways to check the device, each carrying specific risks:

- Checking for warning signals (see the “red flags” tool) is the least intrusive way and should be always checked, but also is the least secure.
- Using an antivirus program for mobile devices. Pay attention to the fact that stalkerware may alert the perpetrator that an antivirus program is being used.
- Using specific tools, like TinyCheck. The perpetrator will not be aware that this tool is used, but it requires to have a second prepared device available.

REMEMBER: when checking for unknown apps in the device, please keep in mind that there may be several apps installed by default that are part of the operating system. If you have any doubt, ask a trusted IT tech to help you identify the unknown apps.

The support service may train its professionals on how to check the devices and provide them with checking tools like TinyCheck.

Alternatively, the support service may team up with a trusted IT tech that will check the victims/survivors’ devices.

REMEMBER: a negative check does not mean there is no issue. The perpetrator may be using other means to monitor/track the woman. For example, he may have access to her online accounts, or may be checking her phone without her knowing, etc.

Cyber violence and stalkerware: what to do guide for professionals working with victims/survivors

■ Safety measures when there is the suspicion that the victim/ survivor may be monitored and/or tracked

□ Inform her that stalkerware might register her conversations even if it's turned off. Suggest that she should leave it in the car or outside the room during interviews at the Service or with doctors, police, lawyers, etc.

□ If she has recently received a new phone as a gift, restore factory settings (be aware that this might not work with some stalkerware apps but in many cases, it is successful to remove stalkerware. However, this means that the perpetrator will be alerted as he will lose the ability to monitor the device.)

□ Check if internet data usage has increased without reason (it is also possible to install apps to monitor this in the future)

□ Install an antivirus app (REMEMBER: as we mentioned, stalkerware apps can alert the perpetrator that an antivirus has been installed)

□ Change passwords of devices and accounts frequently, using passwords that cannot be easily guessed

□ Change the phone's unlocking method; use PIN or sequence instead of fingerprint and facial recognition

□ Check apps location and camera permissions and revoke them if they are active

□ Disconnect WhatsApp Web and/or Telegram from PCs and other devices that can be accessible to the perpetrator

□ Discuss with the woman the importance of not letting her children use her devices.

□ Change online banking access account

□ Ask a trusted mechanic to check and possibly deactivate the car's GPS

□ Tell her not to accept friendship or follow requests from strangers

□ Check the list of followers/ friends in every social media and unfollow/unfriend unknown profiles. Remember that if the profile/account is public, everyone can see its content without being a follower/friend

□ Tell her not to share on social media and on WhatsApp stories pictures or other details that may reveal information on her whereabouts

□ Explore the possibility that the woman may have other seemingly innocent accounts shared with the perpetrator (see list below)

Cyber violence and stalkerware: what to do guide for professionals working with victims/survivors

Safety measures when it is certain that a phone/device is tracked

When it is certain that a device is tracked through a stalkerware app or that the perpetrator is monitoring the victim/survivor through other IT means, it is important to take the necessary steps to ensure the safety of the victim and the collection of evidence against the perpetrator.

□ If a stalkerware app is detected, the victim/survivor will want to get rid of it immediately. Explain to her the consequences of uninstalling it (escalation of abusive behavior, destruction of evidence)

□ Review and strengthen the IT safety plan

□ Remember that resetting the device to factory settings will destroy evidence and may not be effective on older phones

□ Help the victim/survivor activate a new SIM card and find a safe device

□ When installing apps on a new device or on the old one after factory reset, download the apps directly from the store and not from a backup because it could download the stalkerware app again.

□ Create a new Google or iCloud account for the safe device

REMEMBER: creating new Google or iCloud accounts to activate a safe device is a fundamental step in IT safety planning, because these accounts give access to a wide variety of apps and information, like emails, files on cloud storages, maps and locations, photos, contacts, etc.

□ If there is no stalkerware, but the perpetrator is monitoring the woman through other IT means (e.g., he has access to her online accounts, etc.), collect data on what accounts/data are being monitored

□ Even if the victim/survivor is not sure if she wants to involve the police, suggest that she keeps a log of incidents (including date, time, location, witnesses (if any), suspected technology involved (e.g., phone, email, etc.), and a brief description of what the abuser did)

□ Remindher to change passwords only when it is safe to do so.

□ Talk about how to use the tracked device / accounts in an organized and controlled way, in order to avoid giving too much information to the perpetrator but, at the same time, without raising his suspicions

Cyber violence and stalkerware: what to do guide for professionals working with victims/survivors

■ What to do in case of cyber-harassment or non-consensual sharing of pictures or information

In case of suspect or certainty about these forms of cyberviolence (that include sextortion and revenge porn), aside from the importance of reporting them to the police (Cyberbullying, revenge porn and non-consensual sharing of explicit sexual images and videos are illegal in Italy, and can be reported within 6 months from the fact)
These forms of cyberviolence, including sextortion and revenge porn, are illegal in many countries across the EU and it is important to report them to the police.

In case of suspect or certainty about these forms of cyberviolence, you can guide the victim/survivor through the following tips and measures to prevent further damages and collect evidence:

☐ It is important to increase the privacy levels of social media accounts, that should be set to the highest level possible

☐ It is possible to set up **Google Alerts** to monitor if content related to the victim/survivor is shared online. Google will send an email when certain terms – like for example the woman's name – appear in Google Search.

☐ To keep evidence of harassment on social media, the first step is to take screenshots of the harassment/abuse. Remember that screenshots do not constitute definitive evidence in court and that digital evidence needs to be acquired too.

☐ Discuss about reporting the harassment/publication of images to the social media (please check each social media's reporting policy **Facebook** | **Instagram** | **Twitter** | **YouTube** | **TikTok**) or website company. If it violates the site's terms of service or content guidelines, they may remove the content. In this case, it is important to document the abuse first to keep evidence of it. Please check below how to report to adult websites.

☐ Sometimes the same content might have been published in more than one place. In this case, search engines "reverse search" function can help. To "reverse search", you will need to upload the picture to the search engine, that will scan the web to see if it's been published somewhere. Please be aware that this process can be very distressing fort the victim.

☐ In case of harassing phone calls, these can be recorded and kept as evidence.

⚠ WARNING: be sure to check if your country's privacy legislation allows the recording of phone conversations without the other party knowing

☐ In case of phone number/ caller ID impersonation (spoofing), it is important to document call logs by taking a photograph/screenshot of the Caller ID and registering the date and time of the calls, as well as phone records to show the number of the originating call, date, and time.

Cyber violence and stalkerware: what to do guide for professionals working with victims/survivors

□ If content has already been published, it can be removed from search engines: EU residents have the right to request that links to pages containing data that is out of date, irrelevant, excessive or inaccurate must be removed from **Google** search results. It does not require those pages to be taken down, only that they not be shown in Google's search results, reducing the chance of people finding it. This can also be requested to **Bing** and **Yahoo** (there might be a different link for each country).

□ Monitoring comments and feedback when pictures/videos have already been published can cause more distress. Suggest to the victim that she tries not to monitor the content online and resulting comments.

□ If the perpetrator has threatened to publish private content on Facebook and Instagram, you can help the victim/survivor accessing **Facekook's Pilot NCII program** . This program can prevent certain images from being published. The victim/survivor will have to contact one of the Pilot's partner organizations (see **list** here) and provide the original picture (not the screenshot) to be blocked.

■ Removal of content from adult sites

If private content has been published online on adult sites, most websites have a "content removal" policy. Here you can find the "content removal" page for some websites **Pornhub** | **Xhamster** | **X videos** | **XXNX** (attention: these links will open the adult sites page)

Safety tips for reporting

□ When making reports, use private browsing mode

□ Do not use a personal email address (create one for the purpose)

□ Do not provide a copy of your ID if the websites request it

□ Provide the exact URL of the video or picture you want to take down

□ Request that all videos and pictures, including thumbnails, are removed

Cyber violence and stalkerware: Technology and social media safe tips for survivors

Technology is a fundamental part of our lives: it is everywhere, and we use it constantly. It is important to know how we can increase our personal "digital safety" so that we can continue to use technology and stay connected.

Here you can find some tips on how to improve your digital safety while you still live with an abusive partner or after leaving him.

☐ **Use a safe device**, that is, a device that your partner can not access. It can be a new device, a public one, or a trusted person's. You should use this device for all the information and communication that your partner must not know. This includes communications with the support service, with the police, with your lawyer, with your doctor, online banking, etc. An old mobile phone without data connection is also a good choice. **Activate a new phone number**: or use a safe number to communicate with the police, the support service, and your lawyer. Share this safe number only with trusted persons.

☐ **Add password or PIN to devices**: every device that you have – phone, pc or tablet – should be protected with a password, passcode or PIN that only you know. When you set up these passcodes, do not use birthdates, pet names, or other thing that you like (food, movies, songs) and that can be easily guessed. Do not use the same passcode for every device.

☐ **Do not share passwords** and passcodes with other persons, not even with your children (they might share passwords with their father).

☐ **Do not save passwords** and passcodes on your computer or phone. Browsers like Chrome, Edge, etc. will ask you if you want to memorize your passwords for future use: say "No". If you are already using saved passwords to log in to your accounts, your partner may be able to access them. You can safely store your passwords in dedicates passwords manager apps.

☐ **Set up a new email account** to manage your communications. You will also use this email account to set up other accounts (for banking, health services, insurance, etc.) and when you need another email to verify your identity. If possible, don't use your name/surname for the email, but choose another name (for example *SomethingSomething@email.com* instead of *YourNameSurname@email.com*)

☐ **Create a new Google or iCloud account** for your safe device. Remember that Google or iCloud accounts often store information on you and your life, like photos, emails, contacts, files, etc., so it's important that you choose a strong password to protect your new account and that you don't share it with anyone.

☐ **Deactivate smart home devices** like "google nest" or Alexa, that may be used to listen to conversations from afar.

☐ **Use incognito mode** in your browser when you navigate, so that you leave no trace of the websites you visited.

☐ **Sign off and log out** from sites and accounts, especially social media and email. If you just close the window, someone else using the pc may be able to access your accounts.

Cyber violence and stalkerware: Technology and social media safe tips for survivors

□ **Check privacy settings** on social media and set them to the highest privacy level. Do the same with your children's accounts.

□ **Be careful about what you post online**, avoid posting anything that might reveal your movements, or that may damage your reputation or be used against you. Be aware of who can see your posts and remember that friends and followers can take screenshot of your pictures and posts and share them, with others. As a norm:

- Do not post any personal information (name, address, date of birth, phone number)
- Do not tag your pictures with locations
- Ask your relatives and friends not to post pictures of you or your children and not to tag you in pictures

Be selective with your friends and followers on social media. Only add people that you can trust not to communicate with the perpetrator

Checklist for professionals working with victims/survivors

When it comes to online violence and electronic devices, there are a few red flags that can warn the victim/survivor and the professional of the Support Service about the potential presence of stalkerware or of other forms of cyber violence.

Many times, the victim/survivor may not know about the forms and extent of cyber violence. It is important to be active and screen for the possibility of any form of cyber violence even if the woman shows no concern or expresses such suspicions. A woman may not be aware of what is happening, or she may not consider it an issue.

This tool is not to be considered a list of questions to be asked directly to the victim/survivor, but rather as a collection of “red flags” that may signal the presence of stalkerware or of other forms of control perpetrated using digital means. It’s important to remember that cyber violence is not limited to cyberstalking, but it includes other forms of violence, like cyber harassment, non-consensual sharing of images (to the extent of sextortion and revenge porn), trafficking, etc.

The tool provides a list of warning signs divided into four groups:

- Technical aspects regarding smartphones (or other devices)
- Use of devices and accounts
- Behaviour of the perpetrator
- Social media

For each warning sign, you will find the related danger, the possible type of cyber violence and a tip on what to do.

⚠ WARNING: before taking any countermeasure listed below, the priority is to develop a clear and thorough IT safety plan with the woman (see above) Always remember that abrupt changes can escalate the perpetrator’s abusive behaviour

Technical warning signs related to smartphones or other devices

RED FLAGS	Yes	No	Danger	Form of cyberviolence	If yes, what can be done?
The mobile device disappeared for a period of time and then suddenly reappeared			These are signs that a stalkerware app might be installed on the device	Cyberstalking, stalkerware	Check for any stalkerware app installed by the perpetrator. If the presence of stalkerware is confirmed, plan next steps carefully. Please remember all safety issues related to the management of stalkerware
The mobile phone / tablet / pc is also used by the partner					
The phone battery drains faster than before					
There is an app icon that the victim/survivor doesn't recognize					
The phone has a higher consumption of mobile data					
The perpetrator gifted new devices to the victim/survivor or to the children					
In the phone there's an app called "Superuser" (Android) or "Cydia" (iOS)			These apps allow the installation of software bundles on phones		
Some apps have permissions for location and / or camera even if they were not initially set			There may be apps sharing info on location, or using the camera without the woman being aware	Hacking, cyberstalking, non-consensual sharing of images	Periodically check that permissions are revoked
The woman recently changed her mobile phone without deleting the data on the old one			The perpetrator may have access to the old phone, to the data stored there and to apps accounts (email, social media, etc.)		Delete all data from old devices

Warning signs regarding the use of devices and accounts

RED FLAGS	Yes	No	Danger	Form of cyberviolence	If yes, what can be done?
The devices have no unlock protection, or device/account password are simple and the same for different accounts			The perpetrator may have access to the device or to various online accounts	Cyberstalking, Non-consensual sharing of images	Change passwords regularly, choosing complex passwords
Passwords are memorized on a pc / device accessible to the perpetrator					
The woman uses fingerprint or facial recognition to unlock the device			The perpetrator may be able to unlock the device while the woman is sleeping		Change screen unlock option to PIN or pattern. Remember that a PIN code is not always safe either, as it can be easily seen
Messaging apps like Whatsapp Web or Telegram are installed on PCs or tablets accessible to other persons			The perpetrator may be able to read conversations and see photos and video		Disconnect and revoke access to messaging apps (this can be done from the mobile phone). Avoid using these apps on shared devices.
Partners exchanged social media passwords/ accounts					Change passwords
The device is also used by the couple's children			The father could ask the children to report to him the content of messages on their mother's phone	Monitoring, cyberstalking	Change passwords and prevent children from accessing their mother's accounts
The partner has access to the woman's bank details			The perpetrator can check bank movements and authorize money transfer	Cyberstalking, economic violence	Change online banking login data
The woman's car has an integrated GPS system			The perpetrator can track the victim/survivor's destinations and routes	Tracking, cyberstalking	Talk to a trusted mechanic about the possibility of turning off the car's GPS function
The perpetrator has access to the woman's Google account			Through a Google account, the perpetrator can track the location of the woman's Android phone at any moment, as well as check the location history (Google maps timeline)		Turn off "Location history" on the phone, change password.
There are smart devices at home (for example Alexa, Google home, Google nest, etc.)			These devices can be hacked to listen to conversations from a remote location //cyberstalking	Monitoring, cyberstalking	Deactivate the devices, or at least be very aware of their presence

Warning signs regarding partner / perpetrator’s behaviour:

RED FLAGS	Yes	No	Danger	Form of cyberviolence	If yes, what can be done?
Sometimes the perpetrator knows pieces of information that were not discussed or shared with him			The perpetrator may be monitoring the victim/ survivor’s phone, or has access to her media accounts	Monitoring, stalkerware	Check the device for stalkerware
The perpetrator has been spotted at places that the woman doesn't usually go to, without her sharing her whereabouts with him			The perpetrator may be tracking the woman’s phone or car	Tracking, stalkerware	Check the device for stalkerware, deactivate car’s GPS
He quotes parts of messages / phone conversations that the woman had with other persons			The perpetrator may be monitoring the woman’s phone, or has access to messaging apps or accounts	Monitoring, stalkerware	Check the device for stalkerware, change accounts passwords
She is sure that he isn't following her, but she thinks that her partner knows her whereabouts too well			The perpetrator may be monitoring the victim/ survivor’s phone	Tracking, stalkerware	Check the device for stalkerware
The woman’s partner stopped asking to see her phone or to have her passwords			The perpetrator may have installed stalkerware on her phone		
He wants to have sex in the same spot of the same room in particular conditions			There may be recording devices hidden in the room	Non-consensual sharing of images, doxing, sexting, revenge porn, sextortion	Check for recording devices, if possible, cover them with clothes

Warning signs about social media:

RED FLAGS	Yes	No	Danger	Form of cyberviolence	If yes, what can be done?
The woman has been contacted by strangers on social media			The perpetrator may have created fake profiles to monitor her; her contact info may have been shared online by the perpetrator	Monitoring, online harassment, sexting, doxing	Check the unknown profile for pictures, posts, followers, common contacts
She often shares pictures and details on her whereabouts on social media or WhatsApp stories			These details can be used to track and monitor her. WhatsApp stories can be viewed even by someone who's not among her contacts	Monitoring, cyberstalking, non-consensual sharing of images	Talk with the victim/survivor about the importance of evaluating the impact of what she posts
She shared social media accounts passwords with her partner			The partner can access her accounts, monitor conversations, see friends/followers, acquire pictures		Change passwords. Discuss the importance of not sharing them with other persons, not even for "emergency" situations.
The password recovery email address is also accessible to the partner			In this case, if the woman changes a password, the perpetrator will easily find out. He can also change passwords himself, locking her out of her own accounts	Monitoring, cyberstalking, identity theft	Modify the recovery address before changing passwords
The woman noticed strange activity on her social accounts as if someone has accessed them			Someone, not necessarily the partner, may have access to her accounts	Cyberstalking, identity theft, non-consensual sharing of images	Change passwords
The woman has received "appreciation" calls and/or messages from strangers			It is possible that the woman's contact details, and intimate images have been published online	Doxing, sexting, non-consensual sharing of images, cyber harassment, revenge porn	Keep a track of calls/ messages, set up "Google Alerts", request removal from search engines
The woman receives phone calls from numbers in her contacts, but when she answers she finds out it's the perpetrator			The perpetrator may be using apps that fake his caller ID	Spoofing, harassment	Keep a log of these calls together with phone records