



DeStalk TOOLKIT

for practitioners working with perpetrators



DeStalk Toolkit for practitioners working with perpetrators

Content

Glossary of cyber violence terms	3
Cyber stalking	4
Cyber harassment	4
Non-consensual sharing of intimate content	4
Limiting tech access	5
Other forms.....	5
Cyber violence and stalkerware: Checklist of red flags and questions to detect possible episodes of digital violence	6
Technical warning signs related to smartphones or other devices	7
Group session for perpetrators: cyberviolence	10

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

i **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 EIGE¹ 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 \(europa.eu\)](https://www.eige.europa.eu/cyber-violence-against-women-and-girls)

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, messages 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.
- **Gender trolling.** 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 foment 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. Images/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: Checklist of red flags and questions to detect possible episodes of digital violence


When working with perpetrators, both in individual and group settings, you may hear some statements that are in fact red flags that may warn you about the risk of cyber violence being perpetrated.

It's important for you to be able to pinpoint these red flags, to

- Recognize the forms of cyber violence associated
- Further investigate the abusive behaviour connected to cyber violence and assess the risk

In this tool we will specifically refer to cyber violence within a relationship, that is when a man uses technology to

- Control or spy on his partner, using specific apps installed on her device, or accessing her devices and accounts
- Blackmail or threaten her to share intimate images online
- Share or publish online intimate pictures or videos without her consent
- Steal her identity, make debts in her name
- Create fake online profiles to control or spy on her
- Send her threatening and/or offensive messages, also using fake identities/profiles

 **WARNING!** We must be very careful when we talk about cyber violence with perpetrators because we don't want to give them too many details on aspects they don't know about. The risk is to suggest them new forms of coercive control, increasing the risks for victims/survivors.

We recommended to start with general questions and then move to more specific questions about the possible use of violence. This technique is known as funnel questions.

If the program implements "partner contact" activities, or if there's a collaboration protocol with a Support Service for Victims, it's important that all professionals involved in the case share any useful information on possible or actual cyberviolence episodes, in order to better focus the work with the perpetrator and to increase the safety of the victim/survivor. Remember that the exchange of information must be compliant with all privacy regulations.

In the following table you will find some of the red flags associated with cyber violence, together with an indication of the possible type of violence connected, and example questions that can help you get a better insight in a safe way.



Technical warning signs related to smartphones or other devices

 RED FLAGS	Yes	No	Form of cyberviolence	Possible questions
He talks about a shared use of phones and other devices (<i>"she uses mine too, I'm not jealous"</i>)			Cyberstalking, stalkerware	<ul style="list-style-type: none"> Do you think that in a relationship it's important to share everything and that there should be no secrets? Do you get angry if your partner doesn't want you to see her phone or pc?
He says devices or accounts are not password protected, or that he knows the passwords, or that he has access to the password recovery email (<i>"it is a normal thing, if you have nothing to hide..."</i>)				<ul style="list-style-type: none"> Do you get angry if your partner sets up or changes passwords of accounts and devices without sharing them with you? Have you ever glanced at message notifications on your partner's phone? Have you ever checked your partner's phone or accounts without her knowing?
He has recently bought a new device for his partner (maybe to replace a device he broke during an episode of violence; <i>"I got angry and crashed her phone, but then I bought her a new one..."</i>)				<ul style="list-style-type: none"> Why did you decide to give her this present? Do you expect your partner to give you free access to the devices you buy her? Do you get angry when she doesn't answer your calls or messages?
He uses parental control apps (<i>"I use this app to check where my kids are / what they post online"</i>)				<ul style="list-style-type: none"> Why did you decide to use this app? Does your partner know or agree? Have you ever used this kind of apps for other purposes?
He says that he is the person in charge of buying/setting up devices in the family (<i>for example because his "partner doesn't know a thing about technology, I do it all myself"</i>)				<ul style="list-style-type: none"> Why do you have this role in the family? When you deal with these tasks have you ever gotten access to information (on your partner or children) that you didn't have before?
He mentions that his (ex) partner is very private about her phone (<i>"she doesn't want me to look at her phone, she must be hiding something..."</i>)				<ul style="list-style-type: none"> Do you think it is your right to look at her phone? Do you get angry when she doesn't want you to look at it? Have you ever taken it when she wasn't paying attention?
He mentions that the children help him installing apps or that they have access to their mother's devices				<ul style="list-style-type: none"> Have you ever asked your children to report to you information from their mother's device? Have you ever asked them to install apps on your (ex) partners device without her knowing?
He is the only one in charge of managing money at home, or that she is not good at managing money (<i>"she spends all the money, I need to see where it goes"</i>)				<ul style="list-style-type: none"> Do you ever check her expenses? Do you have access to her online banking account? Have you ever made important expenses without her knowing? Do you use other apps to manage your family? (e.g. health, insurance, etc.)



DeStalk TOOLKIT

for practitioners working with perpetrators

RED FLAGS	Yes	No	Form of cyberviolence	Possible questions
He says her new car has a GPS system			Cyberstalking, Tracking	<ul style="list-style-type: none"> Do you think GPS is an important feature of the car? Have you ever checked the destinations on the GPS?
He bought/ installed smart devices at home (for example, Alexa, Google home, etc.)			Cyberstalking, Monitoring and tracking	<ul style="list-style-type: none"> What can you do with these devices? Can you control them from afar?
He refers information on his (ex) partner that he should not know (<i>"I know for sure that she went to that place/ that she met with that person..."</i>)				<ul style="list-style-type: none"> How did you get this information?
He knows about his partner's movements, even those not usual (<i>"she said she was going to the doctor, but she went to [another place]"</i>)			Cyberstalking, Monitoring and tracking, stalkerware	<ul style="list-style-type: none"> How do you know she went there? Did she tell you?
He quotes in detail parts of texts or conversations the (ex) partner had with someone else				<ul style="list-style-type: none"> How did you get this information?
He mentions that his (ex) partner's WhatsApp web/Telegram access details are saved on a shared device			Cyberstalking, Monitoring, (acquired pictures can be shared online or used for sextortion, revenge porn), identity theft	<ul style="list-style-type: none"> Do you ever read your partner's or your children's messages? Do you look at their pictures or check their contacts?
He says he uses social media frequently (more than normal); he often mentions things or images his (ex) partner posted online (<i>"I saw her pictures at [place] with", "she blocked me..."</i>)				<ul style="list-style-type: none"> Do you often check your (ex) partner's profiles? (if she blocked him) Have you ever created a fake profile?
He mentions that he prefers to have sex always in the same spot of the room or in particular conditions (hidden cameras)				<ul style="list-style-type: none"> Why is that? Does your partner share the same preferences? Does your partner know?
He mentions sexting with his (ex) partner (<i>"we send each other pictures"</i>)			Non-consensual sharing of images, doxing, sexting, sextortion revenge porn	<ul style="list-style-type: none"> Have you ever shown the pictures to someone else? (if he "only showed to friends") How? From your phone? Did you share the pictures with them? Have you ever threatened your (ex) partner to publish the pictures? Have you ever shared or published them to get revenge (after a breakup)?



DeStalk TOOLKIT

for practitioners working with perpetrators

RED FLAGS	Yes	No	Form of cyberviolence	Possible questions
He likes to take intimate pictures or videos			Non-consensual sharing of images, doxing, sexting, sextortion revenge porn; digital voyeurism	<ul style="list-style-type: none"> • Is your partner aware of this? • Have you ever shown the pictures or videos to someone else? • (if he “only showed to friends”) How? From your phone? Did you share the pictures with them? • Have you ever threatened your (ex) partner to publish the pictures? • Have you ever shared or published intimate pictures of your (ex)partner to get revenge after a breakup?
He mentions that he frequently watches porn online				<ul style="list-style-type: none"> • Does your partner know? What does she think? • Have you ever shared content with these websites/channel?

Group session for perpetrators: cyberviolence

■ Goals

- Help stop online control and coercion behaviours
- Have perpetrators take responsibility and face the consequences their behaviour has for their (ex-)partner
- Prevent further cyber violence
- Raise awareness on the legal consequences (fines, etc.) connected to cyber violence.

■ Case study

Read or role-play the following case:

“Mark and Lucy have been living together for six years and have a one-year-old daughter. Mark has always been very protective of Lucy, even more so since their daughter was born. A few months ago, Mark asked Lucy to share her phone and PC passwords as he might need them “in case of emergency”. Lucy was doubtful because she was afraid, she would give up some of her privacy, but she trusted Mark and decided to share her passwords. Since then, weird things have been happening: Mark seems to always know where Lucy is or was and he mentioned a conversation she never shared with him. Lucy became suspicious and talked to him about it, also mentioning that she would change her password. He got very angry and blamed her because he thought she had something to hide.

■ Discussion on Mark and Lucy’s story

Divide the group into 3 sub-groups where each of them works on the following questions:

- **Group 1:** Do you think what just happened is violence? If yes, please write on a post-it which one of these behaviours are an indicator of violence.
- **Group 2:** What do you think the effects of this behaviour are on Lucy?
- **Group 3:** Do you think there may be legal consequences for Mark? Which kind?

Discuss the three questions with the whole group

■ Read, reflect, answer and discuss with the group: the forms of cyber violence

Definition and characteristics

Cyberviolence is considered a generic term that indicates all the forms of violence perpetrated through information and communication technologies.

It can be defined as the online access to and distribution of offensive, violent, or dangerous materials with the objective of causing emotional, psychological, or physical damage. The most common kinds are cyber bullying and harassment.

We will talk about online cyber violence within relationships, that is, when someone’s former or current partner uses technology to:

- Monitor or track one’s partner
- Blackmail or threaten her with the release of intimate pictures or videos
- Release intimate pictures or videos
- Steal her identity, or make debts in her name
- Create fake profiles to monitor or spy on her
- Send threatening or offensive messages

Cyber violence within relationships is not separate from “real world” violence, since it often follows the same patterns as offline violence and is associated to both negative psychological and social consequences, including a poorer quality of life, and, often, to physical, psychological and sexual violence (EIGE, 2017).

In fact, social media, smartphones and other technologies can be used to perpetrate violence and this makes perpetrators partners feel paranoid and anxious.

Group session for perpetrators: cyberviolence

Answer these questions

1. Do you think it is important in a relationship to share everything and that there should be no secrets?

never sometimes often

2. Do you get angry if your partner does not want you to see her phone or her pc?

never sometimes often

3. Do ever you check your partner's phone without her knowledge?

never sometimes often

4. Do you get angry when your partner doesn't answer your calls or messages?

never sometimes often

5. Have you ever created a fake social media profile to control your partner?

never sometimes often

6. Do you share your partner's intimate pictures online or with your friends?

never sometimes often

7. Do you check your partner's pictures, messages, location or calls with an app?

never sometimes often

8. Have you ever shared or published online intimate pictures of your (ex) partner to get revenge after a breakup?

never sometimes often

9. Have you ever used your partner's profile or created a fake profile with her name to publish online pictures or other details that could damage her?

never sometimes often

Group session for perpetrators: cyberviolence

Read, reflect, answer, and discuss with the group

Based on what we've seen today, do you think the situations described below can be defined as "violent behaviour"?

Rate each situation on a scale from 0 to 10, where 0 represents a "non-violent" behaviour and 10 a "very violent" behaviour.

The man checks his partner's WhatsApp conversations without her knowing	0	1	2	3	4	5	6	7	8	9	10
The man gets angry because his partner doesn't want him to check her phone; he then accuses her of not loving him enough and of having something to hide	0	1	2	3	4	5	6	7	8	9	10
The man uses technology to monitor her movements, messages, and calls.	0	1	2	3	4	5	6	7	8	9	10
The man creates a fake social media profile to write to his (ex-) partner, pretending to be someone else.	0	1	2	3	4	5	6	7	8	9	10
She sends him intimate pictures or videos, he shows them to his friends or shares them online.	0	1	2	3	4	5	6	7	8	9	10
He threatens his ex-partner that if she doesn't sleep with him, he will post nude images online that she sent him in the past.	0	1	2	3	4	5	6	7	8	9	10
He gets her social media passwords without her knowing.	0	1	2	3	4	5	6	7	8	9	10
He installs the bank app with his partner's data on his phone to check her expenses and earnings.	0	1	2	3	4	5	6	7	8	9	10