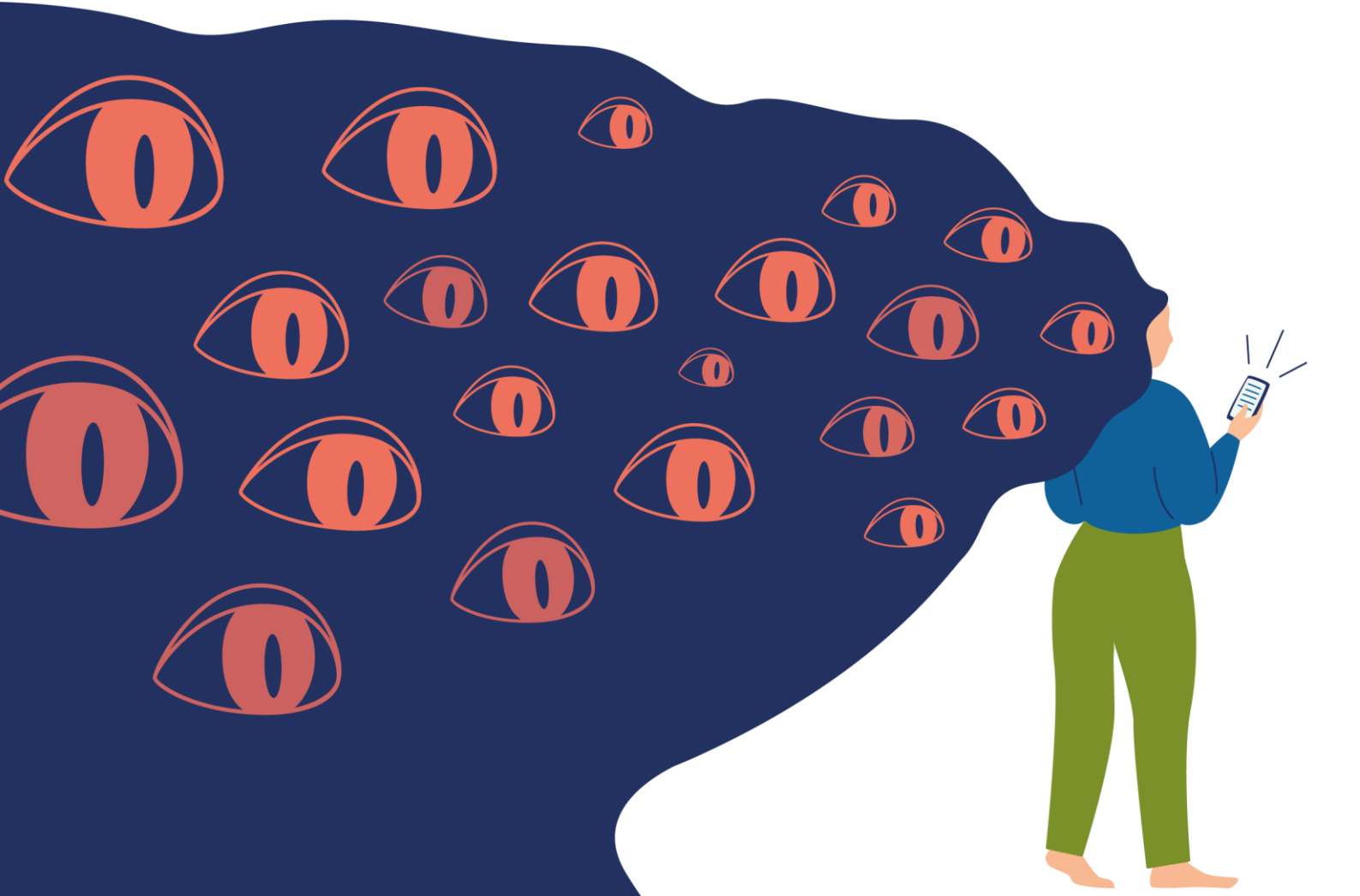


DeStalk

detect and stop stalkerware and cyberviolence against women

Blanquerna
UNIVERSITAT RAMON LLULL

UNA CASA PER L'UOMO
società cooperativa sociale

kaspersky

WWP // EUROPEAN NETWORK

REGIONE DEL VENETO

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

DeStalk

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

WP3 - Capacity building of NGOs and professionals
D3.1 Report on toolkit adaptation

Content

Partner

Una Casa per l'Uomo

Description of the goal

The aim of this task is to define the process that led to the creation of a toolkit to work on cyberviolence and stalkerware with perpetrators and victims of violence

The toolkit adaptation

The process of adapting the existing tools to include cyberviolence and stalkerware was divided into the following phases:

1. Research and collection of existing tools
2. Collection on information on existing best-practice and on knowledge on cyberviolence among EU and Italian organizations
3. Revision of existing tools and creation of new tools

Preliminary work

A the team decided to implement a few preliminary actions to answer the following questions:

- How much do professionals working with victims and perpetrators know about cyberviolence and stalkerware? What about other stakeholders?
- What are the tools that these professionals use to correctly identify this kind of violence?
- What are the training needs on this?

As a first step, the team decided to start mapping the tools already used by the two services run by Una Casa per l'Uomo: "Cambiamento Maschile" (Perpetrators program), and "Stalla Antares" (Victims support center). The tools already in use can be divided into different categories, each one dealing with a different phase of the work with perpetrators and victims:

- Detection of violence
- Risk assessment
- Assessment of change
- Work on violence

After mapping all the tools and materials already in use, the team came to the following conclusions:

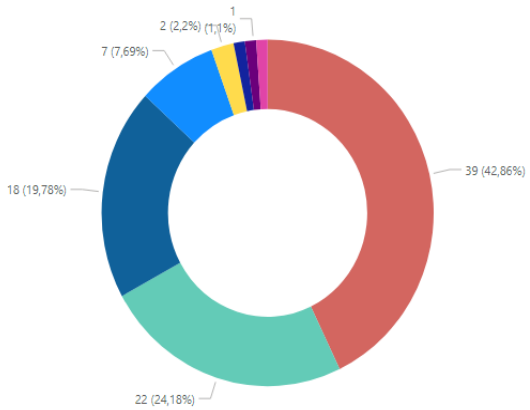
- Even though "new technologies", with all the connected hardware and software, are part of every day's lives of professionals and clients, they are never mentioned in the tools used in the work with victims/survivors and perpetrators (e.g. : case studies used for PP's group sessions never include references to IT or online violence)
- All mapped tools reference the categories of violence defined by the Istanbul Convention (physical, psychological, economical, sexual, stalking), but there is no explicit mention to online violence and /or stalkerware.
- The description of violent behaviours never includes online violence or stalkerware. For example, all examples describing "control" are related to physical coercion, loss of friends and family networks, etc.

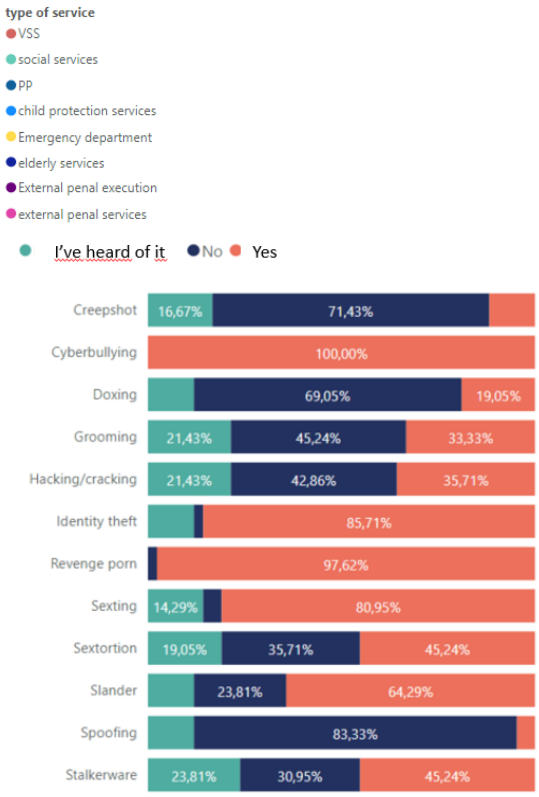
Starting from these considerations, the team decided to extend the research through the following activities:

a) An online survey
b) An online Focus Group for professionals working with victims and perpetrators

The survey

The survey was designed to map knowledge and training on cyberviolence. The survey was addressed to professionals working with perpetrators and victims and to other relevant stakeholders, in Italy and across Europe. The questions were drafted by UCPU's team and revised by all DeStalk partners. The survey was published online (https://bit.ly/DeStalk_Survey) in 5 languages (Italian, English, French, German, Spanish).
The survey had 96 total responses (95% from Italy), with 39 responders from VSS, 19 from PP and 34 from other relevant stakeholders





According to the results of the survey, professionals working with victims/survivors and perpetrators have heard of cyberviolence in general, but often don't know about the specific forms: the most known forms of cyberviolence are the ones that are most often mentioned by media and that have laws addressing the, as Cyberbullying, Identity theft, revenge porn. Other forms like creepshot, doxing and spoofing are widely unknown. Less than half of responders have only partial or no knowledge on Stalkerware.
While professionals working with victims/survivors and perpetrators all consider cyberviolence as very relevant in their work (with a rating of 4,45 out of 5), only 23% of VSS and 37,5% of PP responders attended some form of training on the topic.
The issue of the correct detection and assessment of cyberviolence is made clear by the results of the questions regarding the number of cases, the categorization, and the use of tools: professionals from VSS have encountered cyberviolence cases more than professionals from PP (56% vs 18%).
Regarding the use of specific tools on cyberviolence, only 11% of VSS use them, while 100% of PP have none. When detecting forms of violence, episodes of online violence are categorized

as "stalking" (37,5% of PP and 34,6% of VSS) or psychological violence (31% of Pp and 26% of VSS). Only 1 in 4 PP and VSS have a specific category for cyberviolence. From these sets of data, it appears that cyberviolence may often be misidentified of labelled incorrectly, also due to the lack of specific tools and knowledge, thus leading to the underestimation of the phenomenon.

The focus group

On May 14th, PP and VSS respondents were invited to join the UCPU team to a 3-hour online focus group aimed at:

- Informing the participants about the DeStalk project, its partnership and its actions and objectives
- Giving the participants some basic knowledge on cyberviolence and stalkerware
- Sharing the results of the survey
- Discussing and sharing training needs and experience on existing tools and best practices

The focus group was conducted in Italian by two of UCPU's team members working respectively with perpetrators and victims/survivors. Professionals from 28 different organizations (13 PP, 13 VSS, 5 other) joined the meeting.
The discussion highlighted the following focal points:

- Even though they are aware of the existence of forms of violence that are perpetrated online or through commonly used devices, professionals admit that they do not have specific knowledge and skills on the topic, regarding to both the detection and assessment of cyberviolence and the practical work with perpetrators or victims/survivors. The lack of knowledge leads to the issue of the efficacy of prevention and contrast measures adopted by both types of services.
- even though social media, the internet, mobile phones and other IT devices are part of every day's life, professionals admit a sort of "computer illiteracy": there is still a lack of knowledge and awareness of the effects and even devastating consequences of the incorrect use of the web (e.g. lack of data protection, communication of personal data to other parties, posting of private images online, etc.). This also applies to *digital natives*, as reported by professionals that also work with adolescents in schools.
- Participants agree that cyberviolence and stalkerware have characteristics that need to be taken into consideration in their work, such as:
    - Cyberviolence can be easily perpetrated by most individuals using commons means that also grant the anonymity of the perpetrator
    - Cyberviolence can potentially affect a high number of persons, including specific categories of vulnerable targets (e.g. pre-adolescents)
    - The effects on victims/survivors can be devastating
- Different toolkits on cyberviolence need to be prepared to address the specifics of the work with perpetrators and with victims/survivors
- All participants agree on the need for training and capacity building on cyberviolence and stalkerware, on the use of specific tools, and on a multiagency approach to violence.

The work on the toolkit

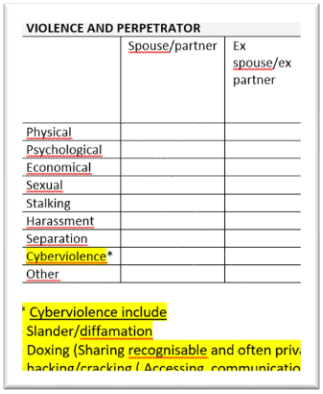
All the preparatory work done in the first two phases helped the team to focus on the following aspects:

- How and through what tools can professionals correctly detect and assess cyberviolence?
- How and through what tools can professionals correctly detect and assess the sub forms of cyberviolence?
- When cyberviolence is detected, what should professionals do to manage the situation? How can they avoid "paradoxical effects" (like for example removing a stalkerware app without taking all the needed precautions)?
- How can tools be differentiated for PP and VSS?

Having these questions in mind, the team worked on the following ideas:

- Detection/assessment tools already used by PP and VSS need to be updated by including
  - Cyberviolence as one of the categories of violence (alongside those mentioned in the Istanbul Convention). This will give a better mapping of the phenomenon
  - The sub-forms of cyberviolence (e.g. sextortion, stalkerware, doxing, etc.) and of the related behaviours.
- Professionals need to have clear indications and instructions on how to deal with cyberviolence, to avoid useless or counterproductive actions
- There needs to be two different toolkits, one for PP and one for VSS, to grant the safety of victims/survivors and to avoid that talking explicitly of cyberviolence with perpetrators may teach them new ways to perpetrate violence.

The adaptation of existing tools



VIOLENCE AND PERPETRATOR	Spouse/partner	Ex spouse/ex partner
Physical		
Psychological		
Economical		
Sexual		
Stalking		
Harassment		
Separation		
Cyberviolence*		
Other		

* Cyberviolence include
Slander/diffamation
Doxing (Sharing recognisable and often priv
hacking/cracking / Accessing communicatio

As mentioned above, the tools that are already used by PP and VSS need to be adapted to include cyberviolence.

- Personal files of victims/survivors and perpetrators
  - "cyberviolence" added as one of the categories of violence, alongside with a brief list of the sub-forms
  - "IT consulting" added as one of the services that can be provided
- Practical tools used during interviews were updated to include items specifically related to cyberviolence. For example, the "questionnaire on violent and controlling behaviours" used during PP individual interviews was updated as follows:
  - In the "Control" section, items on the cyberstalking were added ("You controlled her phone, pc or other devices", "You hacked or controlled her email, WhatsApp, social media")

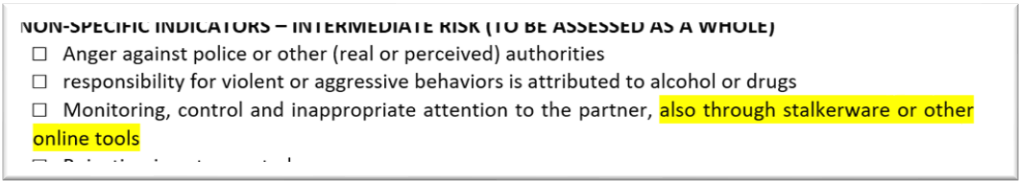
- In the "Physical, sexual, psychological abuse" paragraph, two more items were added ("You shared or published online intimate images without her consent"; "You reply to her online posts with threatening, offensive messages or false accusations")
- In the "coercion and threats" paragraph, "*You threatened her to publish intimate pictures online*" was added

Coercion and threats	How often
You threatened to do something to hurt her	1 2 3 4 5
You threatened to leave her	1 2 3 4 5
You threatened to kill yourself	1 2 3 4 5
You threatened her to publish intimate pictures online	1 2 3 4 5

- ASAP protocol

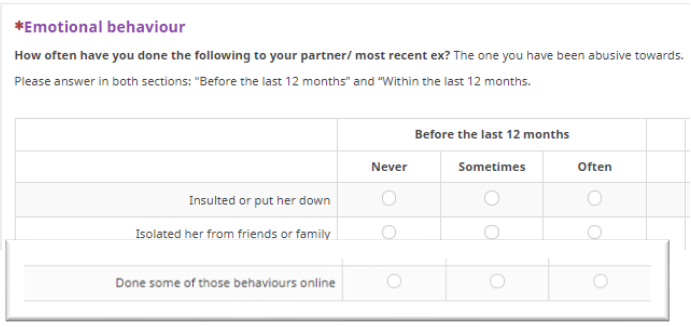
The ASAP protocol was drafted and tested during a previous EU funded project, and it provides guidelines and tools to foster collaboration between PP and VSS. The protocol was amended by introducing cyberviolence both in the introductory part and in the tools.

- The definition of cyberviolence was added to paragraph 1.1 "The Istanbul Convention and the definition of violence"
- In paragraph 4.1 "Phase 1", the sentence "*Agree on definitions, especially related to forms of cyber violence*" was added as one of the topics that need to be discussed and shared by organizations at the beginning of their collaboration
- For the "assessment of recidivism", cyberviolence was included in the list of topics to be discussed
- On the "evaluation of other elements", the sentence "*Case managers should also discuss and share information on any form cyber violence, regardless of if it certain or suspected*". This is especially useful to improve the safety of both the victim/survivor and of the professionals involved.


NON-SPECIFIC INDICATORS – INTERMEDIATE RISK (TO BE ASSESSED AS A WHOLE)
☐ Anger against police or other (real or perceived) authorities
☐ responsibility for violent or aggressive behaviors is attributed to alcohol or drugs
☐ Monitoring, control and inappropriate attention to the partner, also through stalkerware or other online tools

- The "risk assessment checklist "was updated to include one more item in the high risk list ("*He has access to her accounts and devices*") and one item in the non-specific list ("*He has access to intimate pictures or videos of her*"). Other items were modified to include online violence (eg. the item "Monitoring, control and inappropriate attention to the partner", became "*Monitoring, control and inappropriate attention to the partner, also through stalkerware or other online tools*")

- Impact Toolkit


*Emotional behaviour

How often have you done the following to your partner/ most recent ex? The one you have been abusive towards.

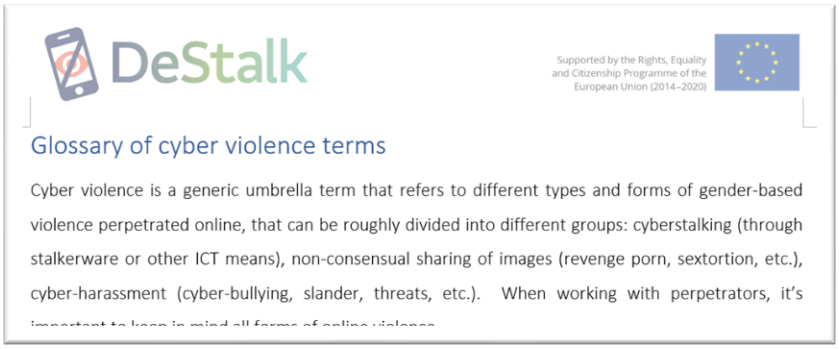
Please answer in both sections: "Before the last 12 months" and "Within the last 12 months.

	Before the last 12 months			
	Never	Sometimes	Often	
Insulted or put her down	○	○	○	
Isolated her from friends or family	○	○	○	
Done some of those behaviours online	○	○	○	

The questionnaire was updated by adding the item "done some of those behaviours online" to the list of emotional violent behaviors

The toolkit for professionals working with perpetrators

The toolkit designed specifically for the work with perpetrators is composed of three parts.
Glossary of cyberviolence, with thorough definitions of all the current forms of cyberviolence. Given the many different forms of cyberviolence, and the lack of a well-defined international nomenclature, it is important that all organizations and agencies that work on cyberviolence share the same definitions.


DeStalk

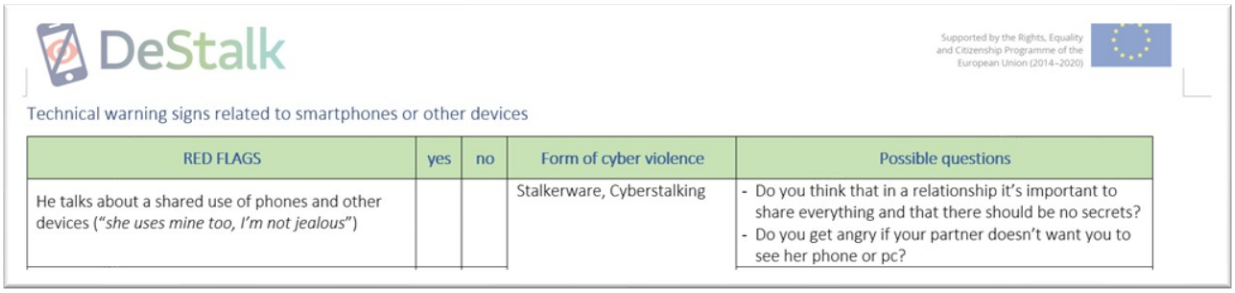
Supported by the Rights, Equality and Citizenship Programme of the European Union (2014–2020)

Glossary of cyber violence terms

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), non-consensual sharing of images (revenge porn, sextortion, etc.), cyber-harassment (cyber-bullying, slander, threats, etc.). When working with perpetrators, it's

Checklist of red flags and questions to detect possible episodes of cyber violence

The checklist is introduced by indications and recommendations for an effective work with perpetrators.
This tool can be used during individual interviews and group session, and it is intended as a reference for professionals, not as a list of questions to be asked directly to perpetrators. The checklist aims at providing professionals with a tool that can help them identify potential forms of violence, categorize them, and investigate them further.


DeStalk

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

Technical warning signs related to smartphones or other devices

RED FLAGS	yes	no	Form of cyber violence	Possible questions
He talks about a shared use of phones and other devices (*"she uses mine too, I'm not jealous"*)			Stalkerware, Cyberstalking	- 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?

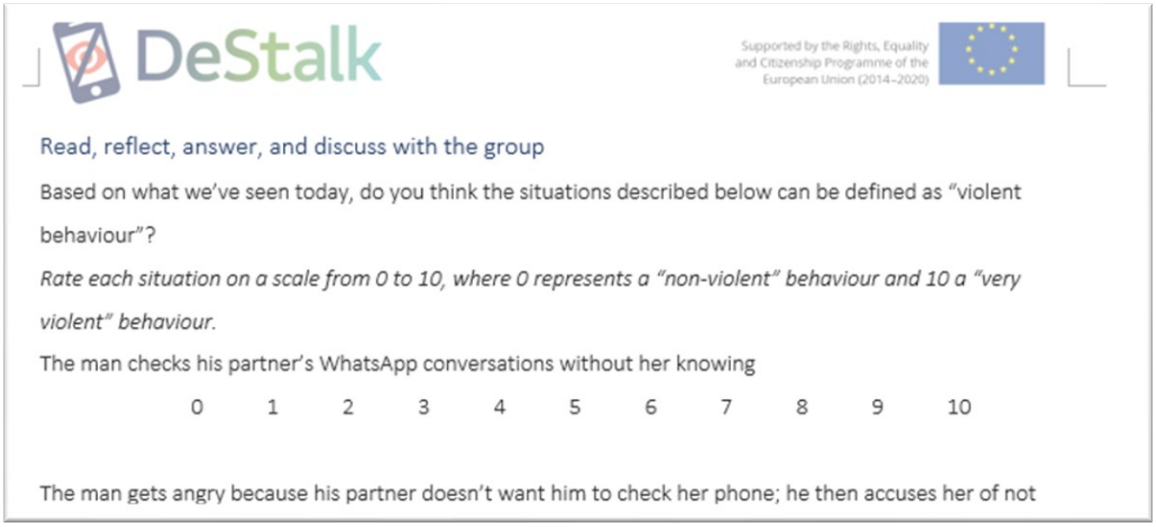
The checklist is a collection of so-called red flags, that is things that the perpetrator might say and that could indicate possible cyberviolence behaviour. For each red flag, the tool provides the relates form of cyberviolence and a list of possible questions that the professional can ask the perpetrator without specifically mentioning cyberviolence (The risk is to suggest them new forms of coercive control, increasing the risks for victims/survivors).

Group session for perpetrators: cyberviolence

This tool is an adaptation of the sessions included in the guide "Same Violence, New Tools. How to work with violent men on cyber violence" (Letizia Baroncelli, WWP EN 2020)
This tool is intended as a session for perpetrators groups. Its goals are:

- Help stop online control and coercion behaviours
- Have perpetrators take responsibility and face the consequences of their behaviour
- Prevent further cyber violence

The session includes case studies, exercises and discussions to work with groups of male perpetrators


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

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

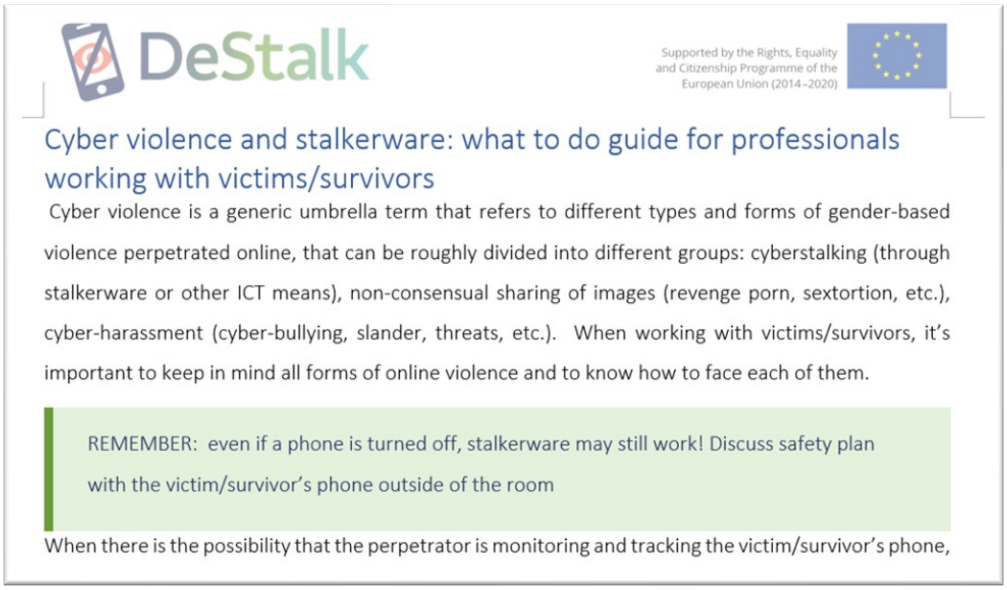
0 1 2 3 4 5 6 7 8 9 10

The man gets angry because his partner doesn't want him to check her phone; he then accuses her of not

The toolkit for professionals working with victims/survivors

While it's important not to give perpetrators too many details on cyberviolence, to avoid suggesting them new ways of perpetrating coercive and violent behaviours, the work with victims is on the contrary centred on the knowledge and awareness of all the ways through which cyberviolence may happen. For this reason, aside from the including in this toolkit the same *glossary* of cyberviolence terms, that as we described above, is particularly important when collaborating with other organizations and agencies, the toolkit for professionals working with victims/survivors include a guide on IT safety planning for professionals, a technology and social media safe tips for victims/ survivors, and a checklist of red flags for professionals.

What to do guide for professionals working with victims/survivors


DeStalk

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

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

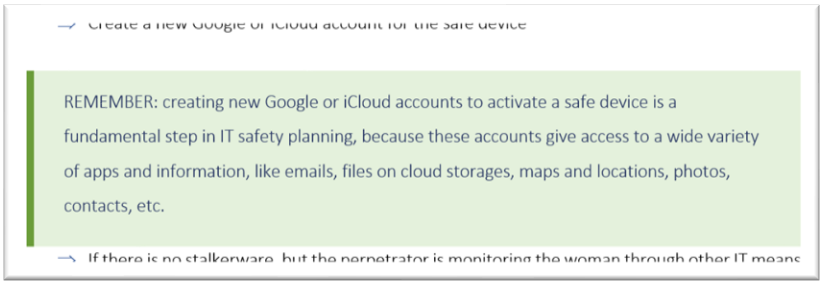
Cyber violence is a generic umbrella term that refers to different types and forms of gender-based violence perpetrated online, that can be roughly divided into different groups: cyberstalking (through stalkerware or other ICT means), non-consensual sharing of images (revenge porn, sextortion, etc.), cyber-harassment (cyber-bullying, slander, threats, etc.). 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.

REMEMBER: even if a phone is turned off, stalkerware may still work! Discuss safety plan with the victim/survivor's phone outside of the room

When there is the possibility that the perpetrator is monitoring and tracking the victim/survivor's phone,

This tool is meant as a practical guide that helps professionals in their work with victims. The guide includes:

- Indications on developing an IT safety plan
- Information on how to check a device for stalkerware
- Safety measures when there is the suspect that the victim/survivor may be monitored and/or tracked
- Safety measures when it is certain that a phone/device is tracked
- Indications on What to do in case of cyber-harassment or non-consensual sharing of pictures or information
- Indications on the removal of content from adult sites


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

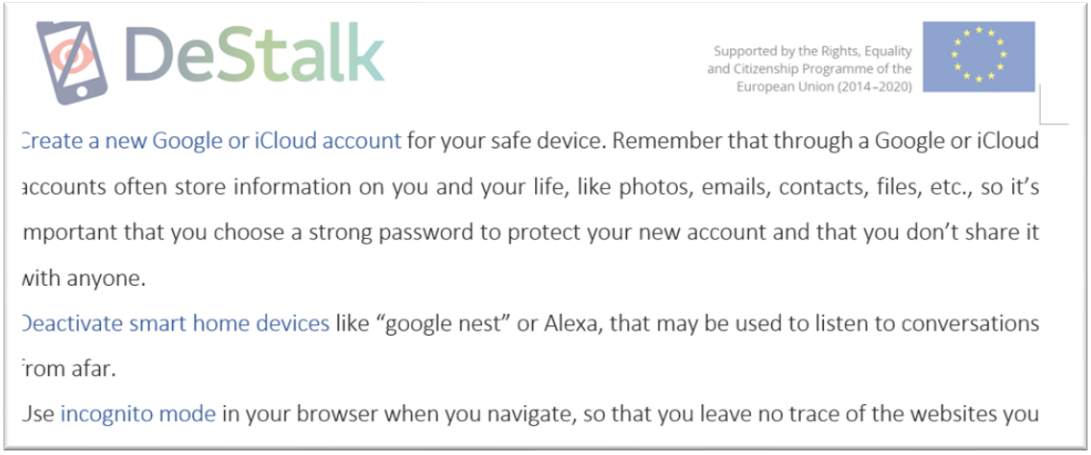
REMEMBER: creating new Google or iCloud accounts to activate a safe device is a fundamental step in IT safety planning, because these accounts give access to a wide variety of apps and information, like emails, files on cloud storages, maps and locations, photos, contacts, etc.

→ If there is no stalkerware, but the perpetrator is monitoring the woman through other IT means

The guide addresses all the main forms of cyberviolence (cyberstalking and stalkerware, non-consensual sharing of images, and cyber harassment) and , when possible, provides links to other tools (for example, a direct link to set up *google alerts)* and to the pages of websites and social media with the description their privacy policies and settings .

Technology and social media safe tips for victims/ survivors

The third tool is a guide specifically designed for victims/survivors with the goal of giving them a few simple indications on how to protect their privacy online and on how to establish and maintain safe communications if their devices are monitored.


DeStalk

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

Create a new Google or iCloud account for your safe device. Remember that through a 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.

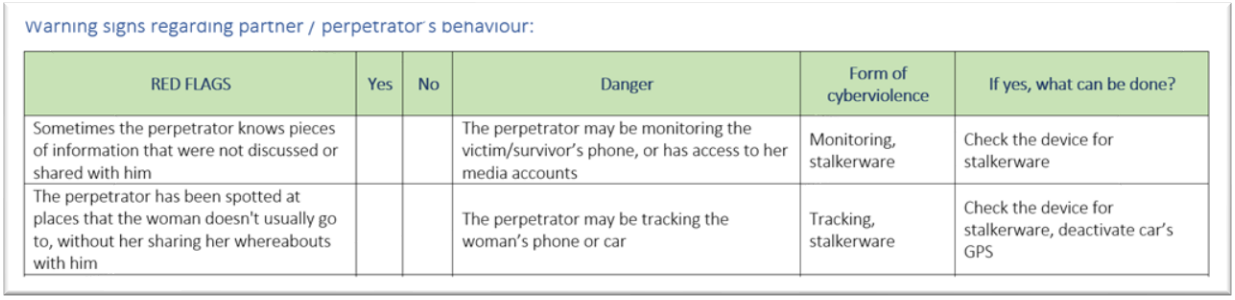
Deactivate smart home devices like "google nest" or Alexa, that may be used to listen to conversations from afar.

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

Checklist for professionals working with victims/survivors

Like the checklist for professionals working with perpetrators, this tool is a collection of red flags that professionals should pay attention to when listening to victims/survivors.
The red flags are divided into four categories:

- Technical warning signs related to smartphones or other devices
- Warning signs regarding the use of devices and accounts
- Warning signs regarding partner / perpetrator's behaviour
- Warning signs about social media


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

For each warning sign, the checklist describes the danger connected to it, the relates form of cyberviolence, and a possible solution. Throughout the checklist, professionals are reminded of the importance of making sure that the victim/survivor is safe before taking any action that may trigger the perpetrator.
The checklist can be used as a reference for professionals, or as a list of questions to ask to the woman.