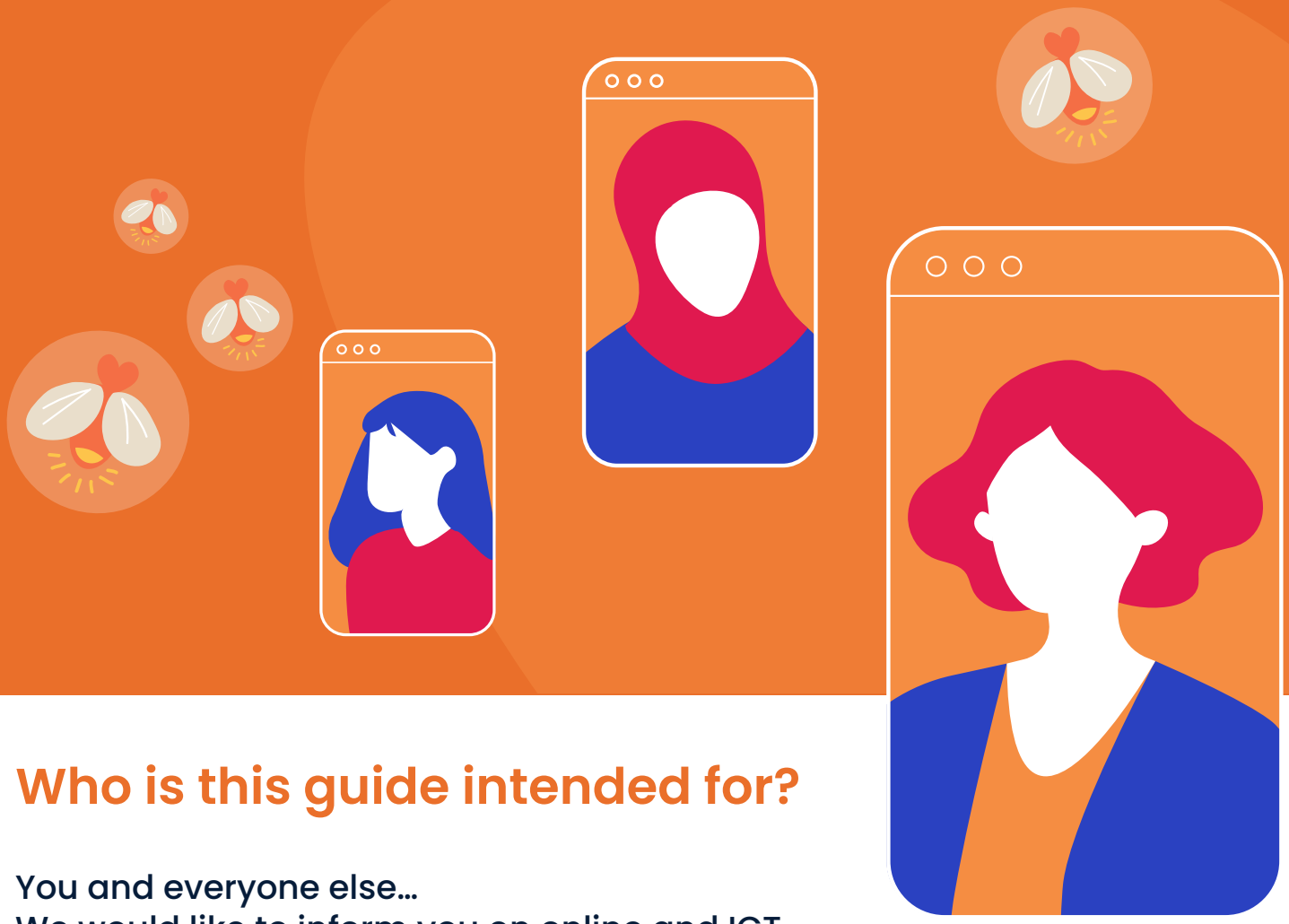
Sweden
Sverige

UN WOMEN

Guide on Gender-Based Cyber Violence



Who is this guide intended for?

You and everyone else...
We would like to inform you on online and ICT facilitated violence (cyber violence) and provide guidance on how you can take the control in the digital environment.

@UNWomenTurkey

Shall we start with the definitions?

Violence against women is a form of discrimination against women and a human rights violation falling under the Convention on the Elimination of All Forms of Discrimination and other international and regional instruments. It includes gender-based violence against women, that is, violence directed against a woman because she is a woman and/or that affects women disproportionately[1].

The definition of online violence against women therefore extends to any act of gender-based violence against women that is committed, assisted or aggravated in part or fully by the use of ICT, such as mobile phones and smartphones, the Internet, social media platforms or email, against a woman because she is a woman, or affects women disproportionately.

Terminology in the area of online and ICT facilitated violence is still developing and there is lack of comprehensive global definition and data. İn this guide, we are using the term "cyberviolence".

The fact that it happens in the digital environment does not decrease the severity of violence!

Very much like all other forms of gender-based violence, cyber violence is a violation of human rights and a result of inequalities!

Around the globe, inequalities have exacerbated during the pandemic and cyber violence has also increased as another form of gender-based violence[2].

Who are exposed to cyber violence?

Everyone!

However, as cyber violence is caused by the same structural inequalities and discrimination which are the root causes of gender-based violence, women and girls are more likely to be exposed, and suffer serious consequences as a result.

It has been estimated that in the EU, 23 per cent of women have reported having experienced online abuse or harassment at least once in their life, and that one in 10 women has experienced some form of online violence since the age of 15[3].

Women face the risk of being exposed cyber violence as well as multiple and intersecting forms of discrimination based on their educational background, age, profession, gender identity, sexual orientation, ethnicity and race, or relationship status.

Women who are more visible in the digital environment are more exposed to cyber violence[4]: women who are politicians, journalists, artists, authors, academics and/or activists may become the explicit target of cyber violence perpetrators at times.

Young people are more digitally active and are particularly exposed to cyber violence.

We know that 94% of young people at the ages of 15-24 are online[5].

UNICEF, in a survey conducted with one million young people, found that more than 70% of the youth at global scale are exposed to cyber violence.[6]

Those who are most exposed to cyber violence in Turkey are between the ages of 25 – 40[7].

Who are the perpetrators of cyber violence?

The perpetrator of cyber violence can be a former or current spouse / partner, neighbor, colleague / peer, a relative or a total stranger.

Cyber violence is not our fault! It is a crime and it is punishable!

Although the perpetrators use different tactics and tools, their objective does not change:

To embarrass, humiliate, frighten, threaten, silence or to encourage the lynching attacks or ill-intended approaches...

Where and how does cyber violence occur?

The acts of cyber violence are committed via Information and Communication Technology (ICT) tools such as social media platforms, messaging applications, Apps, forums, chat rooms of the games and e-mails etc.

The perpetrators are usually very determined to maintain their control, and technology is just one of the many tools they use for this purpose.

If you think that the perpetrator has lots of information about you, s/he may have obtained this information by tracking your devices, accessing your online accounts, tracking your location or collecting online information about you.

Let's elaborate on this topic through some examples...

Cyber violence has many manifestations. Some examples are included here:

The first of them is **cyber stalking.** This is also called "stalking" and sometimes it may not be innocent at all.

Cyber stalking is unwanted surveillance or monitoring of a person by using ICT, namely the internet or other electronic applications and platforms and constitutes a pattern of behavior that causes harm or distress.

Our actions may be tracked and monitored through spywares or keyloggers, spywares that record every keystroke made by a user, without us being aware of it.

Another frequently encountered manifestation is **online harassment.** If we may name a few examples:

- Receiving unwanted e-mails and messages with sexual content
- Inappropriate and aggressive messages on the digital platforms, threats of physical and/or sexual violence

Another manifestation encountered during childhood and puberty is **cyberbullying** .

Cyberbullying is bullying with the use of digital technologies. It can take place on social media, messaging and gaming platforms and mobile phones. It is repeated behaviour, aimed at scaring, angering or shaming those who are targeted[8].

Another manifestation with the most severe impacts is **Non-consensual dissemination of images.**

Non-consensual dissemination of images; is online distribution of sexually explicit photographs and videos without the consent of the person appearing in such visuals.

Generally, the perpetrator is a former spouse or partner who obtained the photographs or videos during the relationship. These images may be used to threaten for not ending the relationship or for certain other demands. The perpetrators do not necessarily have to be a former spouse or partner, a total stranger may access our computers/accounts and use our images as a threat.

Accessing our private data without our consent (hacking our personal accounts, stealing passwords etc.) is a **violation of the privacy.**

If we may name some examples:

- Accessing our photographs and videos without our consent or obtain, use, manipulate, distribute such images,
- Recording, sharing, distributing the private information and contents including (sexual content) visuals, audio clips, video clips without our information and consent,
- Creating a profile on behalf of us using our personal information, also known as "catfishing",
- Searching, collecting and publishing our personal information without our permission and consent, also known as "doxing",
- Reaching to our families, friends, colleagues for the purposes of contacting us or embarrassing us and harassing them.

What are the impacts of cyber violence?

When we are exposed to cyber violence, we may feel "anger, confusion, helplessness, weakness, concerns about our personal safety, fear and sadness" or we may be worried that "our family and friends may learn about it".

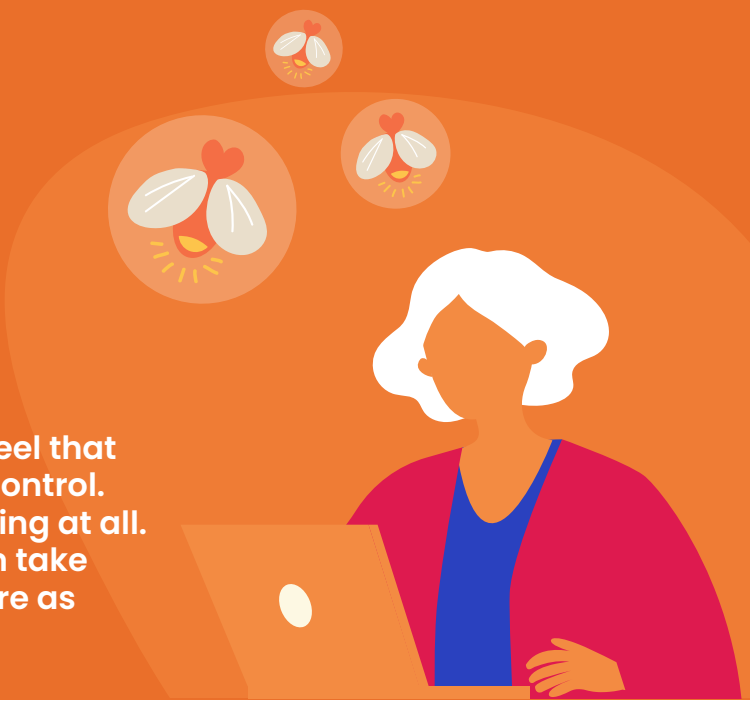
We may trivialize the violence that we experienced, blame ourselves or come to decide that there is nothing to be done to change those things. We may even delete our social media accounts or withdraw from using the Internet altogether.

Deactivating your social media account may seem trivial. However, this pushes women and girls outside digital spaces. Everyone has a right to feeling safe and free in public, private and digital spaces.

The confusion that we have and the state of not knowing what to do is quite normal.

Women are generally exposed to fear, anxiety and depression as a result of cyber violence and this leads to their retreat from online environments. The professional lives and incomes of those exposed to violence are frequently affected and their mobility is restricted. Online forms of violence against women and girls are associated with psychological, social, and reproductive health impacts, and often with offline physical and sexual violence for victims/survivors[9]**.**

How can you ensure your safety?



Being an online target may cause you to feel that things have completely gone out of your control. Sometimes you may not want to do anything at all. However, there are measures that you can take without blaming yourself. Some of them are as follows:

Have confidence in yourself!

You can start by having confidence in yourself and defining what you experienced as violence.

Never forget: It is not your fault! Always remind yourself that you should not blame yourself and there is no justification for violence.

> **The feelings, needs and actions to be taken after an incident of violence may vary from one person to another!**

You can share it with someone you trust and you may receive counseling...

You can tell one of your friends, one of your family members or someone else that you trust about what happened and how you feel about this.

It is you who knows best whom you can trust about this.

You can receive counseling from psychologists, lawyers or information technologies experts.

Do something that makes you feel good!

You can spare some time for yourself every day and put some distance between yourself and the online world. You can do something enjoyable by yourself or together with your friends.

Collect evidence!

Document the cyber violence/the incidents that you experienced. You will need these documentations when you apply to legal remedies for complaint. Besides, these documents may help you better understand your conditions and make a safety planning.

Do not forget to take "screenshots". You better have printouts of your screenshots too!

If you decide to make a complaint...

You need to be informed about what rights are available to you.

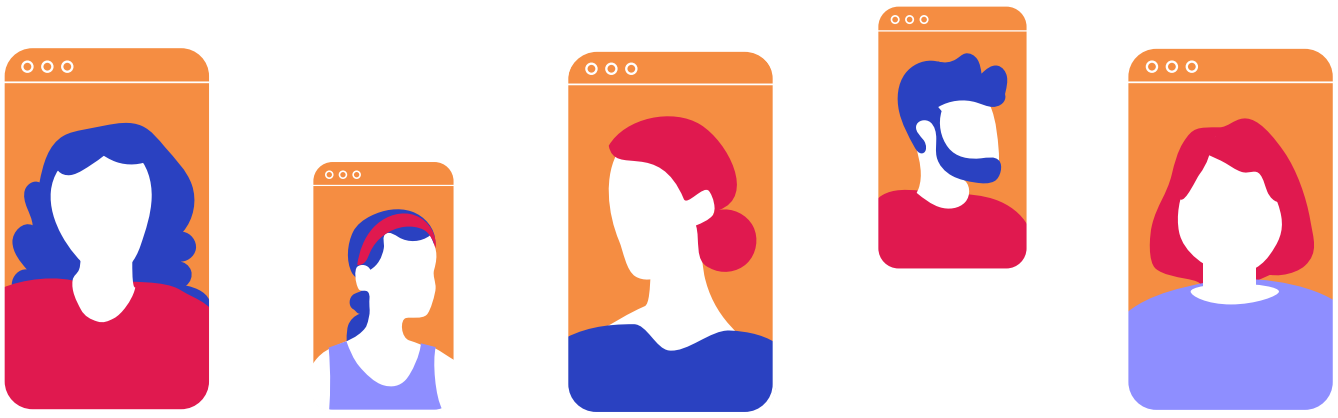
You may talk to the lawyers dealing with these cases or Women Counseling Centers/Commissions of Bar Associations to learn about the legal procedures.

You may make a denunciation at the law enforcement agencies or prosecutor's offices. Make sure to collect all relevant evidence beforehand.

If you decide to report to the relevant authorities, request a person that you trust to accompany you during these procedures.

If the perpetrator is one of your colleagues at workplace, you may report this to the complaint mechanisms of your workplace (ethical board etc.). Make sure that they will secure your confidentiality!

Do not forget that it is your basic right to demand the protection of your personal data and the privacy of your private life.



Gender-based cyberviolence can constitute a criminal act. There are mechanisms defined in national and international laws that you can use against gender-based cyberviolence.

International Treaties:

- **The Convention on the Elimination of All Forms of Discrimination against Women (CEDAW)**
- **The Council of Europe Convention on preventing and combating violence against women and domestic violence (Istanbul Convention)**
- **The Convention on Cybercrime (Budapest Convention)**

What you can do for your and other's digital safety...

We Are Taking Control in the Digital World!

Are your passwords sound and secure?

You should change your passwords periodically and avoid one of the most frequently used passwords in the world[10] and easy to guess such as "12345".
You should not share posts related to the answers to your security questions on the digital platforms.

Using the same password in all platforms will also cause a security gap. Besides, your passwords are personal data and you should not share them with your friends and family members.

Do you use the complaint mechanisms?

When you are exposed to digital violence, you may use the complaint mechanisms of the platform where the incident took place. By doing so, you can ensure that digital platforms become more secure both for you and all other users.

What you have to be careful about using the complaint mechanisms is that you should make the complaint under the relevant topic/section so that the complaint can be evaluated properly. For example, if someone is pretending to be you or someone you know on Instagram and has created an account using your/their photos, you shouldn't make a complaint under "Spam"; instead, you should "Report Account" and mark it "Inappropriate" first and make a complaint under "It's pretending to be someone else" and chose one of the following: "Me/Someone I know/A celebrity or public figure.

Have you fixed your security settings?

You can choose the persons to be authorized to view the e-mail address or telephone number that you give while registering as a member to the digital platforms. Besides, you can also choose whether to be shown among the search results in the platform that you register to. You can even turn off such features as “face recognition” in certain platforms.

All you need to do is to review the security settings of the platform that you register to. When you register to a platform, you better make your security settings before you share anything on that platform.

Have you turned on the two-factor authentication?

Many of the digital platforms have two-factor authentication feature. When you use this feature, they send you a code when a new device is used to log in to your account. This ensures that you log in to your accounts safely when you change a device or a browser.

Do you pay attention to your security in common areas?

When you are in common areas or in a public location, if possible, use your own internet connection instead of shared connections that can be accessed by strangers too. You may even prefer using your mobile phone as a modem (Hotspot) when you need an internet connection for your computer.

Besides, when you log into your account on a computer in common areas, do not forget to log out of all platforms and clear your history in the browser.

Have you authorized any third parties?

You may cause security flaws when you use your accounts in certain platforms to log into applications in digital platforms or to use some features of these applications. For example, you should create a new profile for the platform you are signing up to instead of logging in with your Google, Facebook or Twitter account. You better check the third-party applications that you may have authorized on such platforms and remove the authorization for those not necessary.

Do you share location information?

You better not share your location information when you think that you are susceptible to violence.

Is there an application on your device that you do not know?

You should check your phone and computer and remove any applications not installed by yourself. These applications may be installed on your devices by others to monitor and track you.

Are you sure that you are not click-baited?

The e-mails sent to you might not always have good intentions. The malware, an abbreviation of malicious software, are software that send viruses to collect all the data on your computer when you click on a link in an e-mail or click on or download an attachment of such e-mail.

In order to understand whether an e-mail contains malware, you better check the e-mail address of the sender and the file format of its attachment first.

To see how well-informed you are on phishing:
https://phishingquiz.withgoogle.com

There are things you can do for others!

- You can make a complaint to the social media platforms for the cyber violence that others were exposed to.
- You can send an encouraging support message to someone you know or do not know who has been exposed to cyber violence to let them know that they are not alone.
- The perpetrator may be someone that you know. In that case, if you happen to find yourself making up excuses for the person who has been exposed to violence, question your opinions and never forget that there is no excuse for violence.
- You should not like or appreciate hate speech and sexist discourses and recirculate them by sharing or reposting.
- You had better get consent from persons that you tag in your posts. You cannot know what safety concerns tagging someone in a photo may create for other people!

You can start by sending this guide to your friends...

1 OHCHR (2018). Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective. Available at https://www.ohchr.org/EN/Issues/Women/SRWomen/Pages/SRWomenIndex.aspx

2 UN Women (2020). Online and ICT facilitated violence against women and girls during COVID-19

3 European Union Agency for Fundamental Rights (2014). Violence against women: an EU-wide survey, p. 104.

4 IGF. (2015). Internet Governance Forum-Best Practice Forum on Online Abuse and Gender-Based Violence Against Women

5 ITU (2020) International Telecommunication Union

6 UNICEF (2019). Safer Internet Day UNICEF calls for concerted action https://www.unicef.org/press-releases/safer-internet-day-unicef-calls-concerted-action-prevent-bullying-and-harassment

7 Microsoft (2019). Digital Civility Index/DCI

8 UNICEF (2019). Cyberbullying: What is it and how to stop https://www.unicef.org/turkey/siber-zorbal%C4%B1k-nedir-ve-nas%C4%B1l-%C3%B6nlenir

9 Backe EL, Lilleston P, McCleary-Sills J (2018) Networked individuals, gendered violence: a literature review of cyber violence. Violence Gender 5(3):135–145.

10 Teampassword (2019). Top 50 Worst Passwords of 2019 https://www.teampassword.com/blog/top-50-worst-passwords-of-2019

References:

Temur, N. (2019). Toplumsal Cinsiyete Dayalı Siber Şiddet -Kadın Örgütleri için Rehber

İlkiz, P., Tekin, A. ve Temur, N. (2019). Avrupa Kadın Lobisi- #KadınınİnternetiKadınınHakkı / #HerNetHerRights Türkiye Kampanyası Eğitim Materyalleri

Published by UN Women.
Authors: Nurcihan Temur, Pınar İlkiz

This publication was prepared with the generous support of Sweden through Swedish International Development Cooperation Agency (SIDA). The views expressed in this publication are those of the author(s) and do not necessarily represent the views of UN Women, the United Nations, any of its associated organizations or the official position of Sweden.