Sweden Sverige

UN WOMEN

FOR ALL WOMEN AND GIRLS

MY ONLINE SPACE:

Guide on Women and Girls' Digital Safety

@UNWomenMoldova

Who is this guide intended for?

You and everyone else...

We would like to inform you on digital violence (also called cyber violence) and provide guidance on how you can take the control in the digital environment.

Contents

Shall we start with the definitions? 4

Who are exposed to cyber violence? 4

Who are the perpetrators of cyber violence? 5

Where and how does digital violence occur? 5

What are the impacts of digital violence? 7

How can you ensure your safety? 9

If you decide to make a complaint... 10

What can you do for your and other's digital safety... 11

Are you checking if your phone has been compromised? 14

Glossary 15

Digital Safety Checklist 17

References 18

✊ 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 against Women, as well as the Council of Europe Convention on preventing and combating violence against women and domestic violence (Istanbul Convention).

In the Republic of Moldova, this type of violence is addressed by the Law on Preventing and Combating Violence against Women and Domestic Violence and may be classified as a criminal offence under the Criminal Code. 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 digital 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 technology and social media platforms or email.

Terminology in the area of online violence is still developing and there is lack of comprehensive global definition and data. În this guide, we are using the term ***"cyber violence"***.

> 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 Eastern Europe and Central Asia, more than 50% of women have reported having experienced online abuse or harassment at least once in their life since the age of 18. [3]
>
> In Moldova, a study found that sexual harassment was identified by 41% of the women interviewed as a common form of digital violence, disproportionately affecting women and girls . [4]

Women face the risk of being exposed to digital violence as well as to 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: women who are politicians, journalists, artists, authors, academics and/or activists may become the explicit target of digital 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 at risk of experiencing digital violence in Moldova are young women. A regional study conducted by UN Women in Eastern Europe and Central Asia found that 58% of young women aged 18–24 who were interviewed had experienced online gender-based violence at least once. [7]

☝ Who are the perpetrators of cyber violence?

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

It is also increasingly driven by the growing gender backlash and online groups like the 'manosphere' that spread anti-women and anti-feminist ideas, drawing men and boys into normalizing violence against women and girls.

> Digital 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 or ill intended approaches*

⁉ Where and how does digital violence occur?

The acts of digital 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.

Technology is reinforcing misogynist norms, and online space also fuel misogyny, which means hatred towards women.

For example, the ***"manosphere"*** *— a group of online communities made up of men who spread hate against women — shares sexist content in ways that are easy to spread and hard to stop.*

New tools like artificial intelligence make it easier to spread false information, create fake images, and target women online. The rapid growth of Artificial Intelligence (AI) has further intensified this violence by enabling the spread of disinformation, image-based abuse, and ***deepfake*** pornography.

> 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...

Digital 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 technology, 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 example:

- ***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.***

Cyberbullyingul 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.

Deepfake is a fake video, image, or audio clip made using artificial intelligence to make it look like someone said or did something they never actually did. AI is used to edit women' faces over others' in pornographic videos or photos, seamlessly making it appear as if the intended victim is the person depicted in the video or photos. In fact, studies show that nearly all deepfake content online is pornographic, and about 90% of it targets women without their consent. [9]

Doxing is the publication of private information, such as contact details, on the internet with malicious intent. It often aims to expose women, especially journalists and politicians, to harassment, including sexualized abuse. It includes situations where information like addresses and telephone numbers retrieved by a perpetrator is made public to intimidate or harm violating the right to privacy.

> Perpetrator can be a current or former spouse or partner who obtained photographs or videos during the relationship or modified them with the help of AI. These images may be used to threaten for not ending the relationship or for certain other demands.

In some cases, the perpetrator may be an unknown individual or someone known only through online interactions, who monitors our social media accounts or gains unauthorized access to our devices or personal accounts. They may use our images or deepfake content to intimidate or blackmail us.

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";
- ***Reaching to our families, friends, colleagues*** for the purposes of contacting us or embarrassing us and harassing them.

What are the impacts of digital violence?

When we are exposed to digital 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

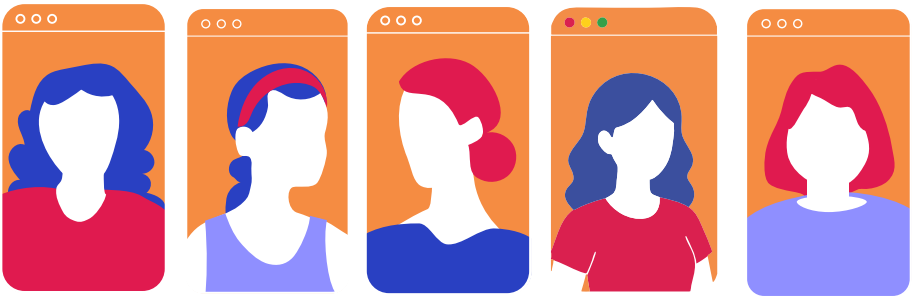
is nothing to be done to change those things. We may even delete our social media accounts or withdraw from using the Internet altogether.

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.

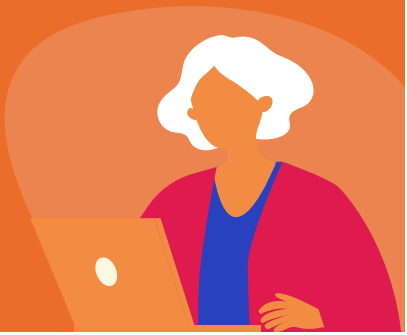
> Women are generally exposed to fear, anxiety and depression as a result of digital violence and this leads to their retreat from online environment. The professional lives and incomes of those exposed to violence are frequently affected and their mobility is restricted.

Online forms of violence against women and girls have ***psychological, social, and reproductive health impacts***, and are often associated with physical and sexual violence in offline settings. [10]



How can you ensure your safety?

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.

> If you find yourself in a situation of online violence or if you just need to talk to someone, you can call the **Trust Line for Women and Girls 0 8008 8008 for support. Your confidentiality is guaranteed.**
>
> If you are concerned about a child or a teenager being affected by online violence, you can anonymously report it using the Sigur online platform on their website – **www.siguronline.md.**
>
> **In case of emergency always dial 112.**

✍ 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 some evidence

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

If you are victim of digital violence as a woman in politics or you are witnessing violence against women in politics online, report the incidents - along with supporting evidence - on the platform ***gender.monitor.md.***

> Do not forget to take "screenshots" or to record some audio if relevant. You better have printouts of your screenshots too or a separate saved file!

⚠ If you decide to make a complaint…

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

- Talk to the lawyers dealing with these cases or women organizations, or if you go to the territorial office of the National Legal Aid Council, you can ask about your rights and legal procedures.
- Call the ***Trustline for Women and Girl at 0 8008 8008*** for confidential support and assistance.
- Make a denunciation at the ***General Inspectorate of Police.*** 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, 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 digital violence can constitute a criminal act. There are mechanisms defined in international and national laws that you can use to protect yourself.

Moldova has joined other countries in Europe and around the globe by ratifying important treaties such as the ***Convention on the Elimination of All Forms of Discrimination against Women (CEDAW)*** and the ***Council of Europe Convention on Preventing and Combating Violence Against Women and Domestic Violence (Istanbul Convention)*** thus committing itself to preventing gender-based violence, including in the digital world.

The laws in the Republic of Moldova establishes criminal liability for several forms of digital violence:

- ***Sharing Private Images:*** Distributing intimate content without consent to humiliate or harm someone's reputation is illegal.
- ***Online Stalking and Harassment:*** Repeatedly contacting or monitoring someone online in a way that instills fear can lead to criminal charges.
- ***Serious Online Threats:*** Frequent threats of a physical, sexual, psychological or economic nature, sent via online platform or electronic devices, are punishable by law.
- ***Technology-facilitated economic violence:*** The unauthorized use of another person's banking information or the withdrawal of funds from the victim's bank cards without their permission.

What can you 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 [11] 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.

> Ana, 25-year-old woman from Chișinău is devastated to discover that her ex-boyfriend has shared intimate photos of her on Instagram and Facebook—without her consent. What was once private has been turned into public humiliation. She feels exposed, violated, and unsure of what to do next.

But she's not alone. Here's what she—and anyone in a similar situation—can do to reclaim control and seek justice:

1. ***Preserve the Evidence***

- Take screenshots of the posts, comments, and the perpetrator's profile.
- If it feels overwhelming, ask a trusted friend to help document everything.

2. ***Report the Content***

- Use the "Report" feature on Instagram and Facebook.
- Flag the posts as "Non-consensual intimate images" or "Harassment."
- Request removal and block the person responsible.

3. ***Contact the Police***

- File a formal complaint with the General Inspectorate of Police.
- Bring all the evidence and explain how this has affected your emotional well-being and reputation.

4. ***Reach Out for Support***

- ***Trust Line for Women and Girls:*** Call ***0 8008 8008*** for confidential, 24/7, and compassionate help.

Have you fixed your security settings

You can choose the person 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.

It's also important to regularly check who follows you on social media and who can see your posts — sometimes, people you don't know, or trust may be following your account. If your profile is public, you may be more exposed and might need to be extra careful.

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. For example, you can control who can see your posts on Facebook, you can restrict followers on Instagram, hide online status on Viber, and select who can contact you on Telegram.

Have you turned on the two-factor authentication?

Many of the digital platforms have ***two-factor authentication*** features. 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. Some social media platforms like Snapchat, Instagram, and Facebook use location-sharing features that can reveal your real-time whereabouts. Ensure you are aware of your location settings both on your phone but also in your app.

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

Are you using these recommended security tools?

- ***Password managers:*** LastPass, Bitwarden, 1Password (free or affordable options)
- VPNs: NordVPN, ProtonVPN, ExpressVPN – ***useful for protecting your internet connection, especially on public Wi-Fi***
- ***Encrypted messaging:*** Signal, WhatsApp (make sure privacy settings are correctly set)
- ***Two-factor authentication:*** Google Authenticator, Authy – adds extra security to your accounts

- ***Removing photo data:*** Photo Metadata Remover – deletes hidden info from pictures
- ***Antivirus software:*** Free and trusted options to protect your device

? Are you checking if your phone has been compromised?

Look for Warning Signs

- Your battery drains quickly
- Your phone uses a lot of mobile data
- It acts strangely (freezes, restarts, or opens apps by itself)

Use These Apps to Check

- ***Android:*** Try apps like Malwarebytes or Avast Mobile Security
- ***iPhone:*** Use Lookout or check for unknown profiles in Settings > General > VPN & Device Management

Where to Get Help

- Ask a trusted tech-savvy friend
- Visit a phone repair shop or cybersecurity support center
- Contact your telephone provider for advice

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...

Glossary

AI / Artificial Intelligence	The ability of machines and systems to acquire and apply knowledge, and to carry out intelligent behavior.
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.
Doxing	Posting personal and sensitive information including home and work addresses, telephone number, email addresses, and family names without permission.
Catfishing	Catfishing is when someone sets up a fake online identity and uses it to trick and control others.
Malware	Malware 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.
Spyware	Spyware is a type of malware designed to steal information by secretly monitoring a user's computer activity
Keylogger	A keylogger is a specific type of spyware that records every keystroke a user types, capturing sensitive data like passwords and bank card numbers, which are then sent to the attacker.
Metadata	Metadata is structured information that describes, explains, locates, or otherwise makes it easier to retrieve, use, or manage an information resource.

Screenshot	A screenshot is an image that you create by copying part or all of the display on a computer or phone screen at a particular moment.
Hacking	Hacking is the act of gaining unauthorized access to data in a system or computer.
Two-factor authentication	Two-factor authentication (2FA) is a way of verifying a user's identity by asking for exactly two pieces of proof, such as the password to an online account (the first factor) and a one-time passcode from an authenticator app (the second factor).
VPN	A VPN is a cybersecurity tool that encrypts your internet connection to hide your location, access content, and prevent hackers intercepting your web traffic.
Encrypt	Encryption is a security method that scrambles data so it is only read by using a key.
Manosphere	A decentralized cross-platform collection of online communities of misogynistic men, amplifies sexist stereotypes in popular, shareable formats that gain traction at scale with limited accountability given the perpetrators' anonymity.
Sextorsion	A type of electronic blackmail, the demand for money, sex/sex acts, or additional explicit images in exchange for not exposing intimate images or private information.
Revenge porn	A form of image-based abuse.

Digital Safety Checklist

„Check Your Online Safety - Monthly Checklist"

- ☐ I have strong passwords on all important accounts (with letters, numbers and symbols together)
- ☐ I've enabled two-factor authentication
- ☐ I've checked my privacy settings on Facebook / Instagram / Tik Tok
- ☐ I've ensured my social media accounts are on private
- ☐ I've reviewed my friends/followers list
- ☐ I've checked authorized third-party apps
- ☐ I'm not posting real-time location
- ☐ I've checked what apps I have on my phone
- ☐ I do not send personal or intimate photos in private messages
- ☐ I do not send money to people I know through social networks
- ☐ I know how to block and report abusive behavior through the apps
- ☐ I know how to report online violence in Moldova
- ☐ I know about women organizations and who to contact in case I need support
- ☐ I know the number of the ***Trust Line for Women and Girls: 0 8008 8008***

References

[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. More 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. More at: https://www.unwomen.org/en/digital-library/publications/2020/04/brief-online-and-ict-facilitated-violence-against-women-and-girls-during-covid-19

[3] UN Women (2023). The Dark Side of Technology-Facilitated Violence Against Women in Eastern Europe and Central Asia. More at: https://eca.unwomen.org/en/digital-library/publications/2023/11/the-dark-side-of-digitalization-technology-facilitated-violence-against-women-in-eastern-europe-and-central-asia

[4] UN Women (2025). Scoping Study for the Chișinău Safe City and Safe Public Spaces Programm.

[5] ITU (2020). International Telecommunication Union. More at: https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2020.pdf

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

[7] UN Women (2023). The Dark Side of Technology-Facilitated Violence Against Women in Eastern Europe and Central Asia. More at: https://eca.unwomen.org/en/digital-library/publications/2023/11/the-dark-side-of-digitalization-technology-facilitated-violence-against-women-in-eastern-europe-and-central-asia

[8] UNICEF (2019). Cyberbullying: What is it and how to stop it. More at: https://www.unicef.org/eca/cyberbullying-what-it-and-how-stop-it#:~:text=It%20is%20repeated%20behaviour%2C%20aimed,or%20threats%20via%20messaging%20platforms

[9] UN Women. (2024). A/79/500 – Ending violence against women and girls: Infographics and recommendations. More at: https://www.unwomen.org/sites/default/files/2024-10/a-79-500-sg-report-ending-violence-against-women-and-girls-2024-infographic-and-recommendations-en.pdf

[10] Backe E. L., Lilleston P., McCleary-Sills J. (2018). Networked Individuals, Gendered Violence: A Literature Review of Cyber Violence. Violence and Gender, 5(3):135–145. More at: https://psycnet.apa.org/record/2018-46721-004

[11] TeamPassword (2019). Top 50 Worst Passwords of 2019.

#NOEXCUSE

for online abuse

Sweden Sverige

UN WOMEN

FOR ALL WOMEN AND GIRLS

This guide was developed by UN Women, with the financial support of Sweden, to raise awareness about the safety of women and girls online and to strengthen efforts to prevent and report digital violence.