UNFPA

UN WOMEN

FOR ALL WOMEN AND GIRLS

Digital Violence/ Technology Facilitated Gender-Based Violence Guide

Who is this guide for?

For you and everyone...

With this guide, we want to give you information about digital violence and help you take back control in digital spaces.

Authors: Nurcihan Temur, Pınar İlkiz
Expanded and Updated Edition – 2025
First Publication: Guide on Gender-Based Cyber Violence (UN Women, 2020)

This guide has been prepared within the scope of the "End Digital Violence Against Women and Girls. Full Stop." campaign conducted by UN Women Türkiye and UNFPA Türkiye. The guide is based on the outcomes of the workshop "Rethinking Violence in the Digital Age," organized with the financial support of the Governments of Norway and New Zealand to ensure conceptual coherence on digital violence.

We would like to thank the civil society organizations and young activists for their support and contributions during the event held on 5–6 November 2025: Alternative Informatics Association, Among Us Gender Studies Association, Damla Göksu, Başkent Youth Council, Beyza Doğuç, Association for Struggle Against Sexual Violence, Havle Women's Association, Hayat Sende Association, Istanbul Bar Association, Istanbul Gender Museum, Kaos GL, Foundation for Women's Solidarity, KızBaşına, UNFPA Refugee Support Services Unit, SGDD-ASAM, SistersLab – Women in Science and Technology Association, SPoD, TED University Gender Studies Center, Federation of Women's Associations of Türkiye, Flying Broom Foundation, ÜniKuir, Zincir Social Enterprise, UN Volunteers: Ada Derya Üstün, Aslı Akbay Alagöz, Elifnur Çağlayan, Elif Sinem Özel.

Shall we start with the definitions first?

Violence against women is defined by many international and national conventions, first and foremost the Convention on the Elimination of All Forms of Discrimination against Women (CEDAW), as a form of discrimination against women and a violation of human rights. Violence against women, to which women are subjected because they are women, is a form of violence that disproportionately affects women.[1]

"Digital violence," or in a broader sense "technology-facilitated gender-based violence," refers to any act that is committed, assisted, aggravated, or amplified by the use of information communication technologies or other digital tools that results in or is likely to result in physical, sexual, psychological, social, political, or economic harm, or other infringements of rights and freedoms.[2]

In this guide, the term "digital violence," which is widely used in Türkiye, is used together with the United Nations' term "technology-facilitated gender-based violence." Since there is no single definition of the concept at the international level, different terms such as "cyber violence," "digital violence," and "technology-facilitated violence against women" are also used in the literature.

- Digital violence is real!
- The fact that incidents take place in digital environments does not reduce the severity of violence!
- Like all forms of gender-based violence, digital violence is also a human rights violation and a result of inequalities!
- By deepening the digital divide, digital violence restricts access to information and services and violates women's right to participate equally in public life!

What distinguishes digital violence from other forms of violence?

Although digital violence shares common features with other forms of gender-based violence (such as being gender-based and widespread), it also has distinctive characteristics related to the nature of the digital environment:[3]

- It can be **anonymous**,
- It can be perpetrated **remotely** (from anywhere in the world without physical contact),
- It is easily **accessible** to perpetrators (low cost and low effort for perpetrators),
- It has a **high speed of spread** (it can spread easily via the internet and re-traumatize those subjected to violence),
- It carries a high risk of **impunity**,
- It allows **automation** (can be automated with limited time and effort),
- It can be **collectively organized**,
- It contributes to the **normalization of violence** (by making violence seem less serious in digital spaces),
- It can be **continuous** (images and digital materials can persist indefinitely).

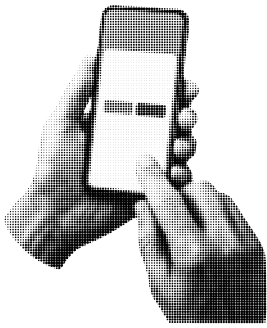
What are the new risks in the digital world?

Rapid technological change is creating new risks and platforms that increase digital violence:[4]

The Rise of Anti-Women's Rights Groups

Some actors who oppose women's rights are using online spaces more and more. This creates a hostile digital environment for women and girls, marked by harassment and threats of violence. Women politicians, women's rights activists, women journalists and women who are visible in public life become direct targets of these attacks.

The Impact of Artificial Intelligence (AI)



The rapid development of artificial intelligence makes it easier to spread misinformation and targeted disinformation. In addition, AI-generated fake images (deepfakes) and non-consensual content are on the rise.

According to Sensity AI data, **90–95 per cent** of fake videos online consist of non-consensual sexual imagery, and about 90 per cent of these target women.[5]

Increase the Misogynistic Attitudes

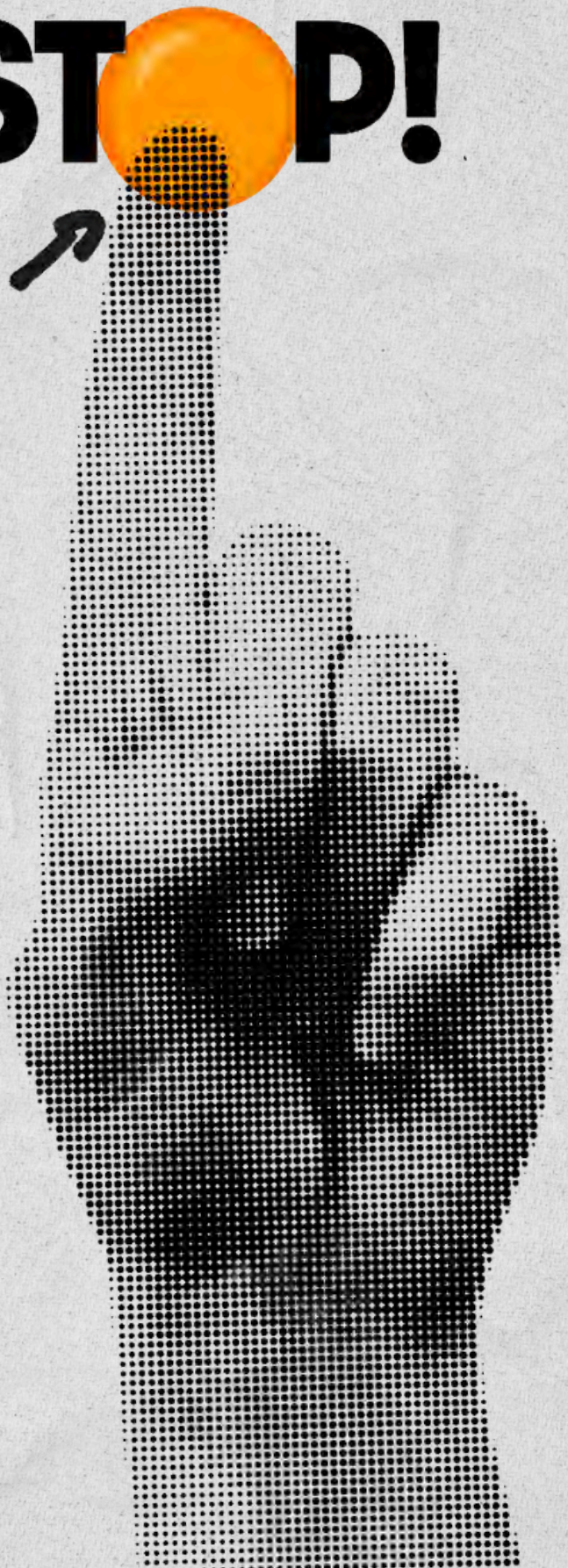
Technology is being used as a tool to strengthen misogynistic social norms. Recent studies show that online spaces fuel misogyny and reinforce the normalization of violence against women.

For example, the network of online male communities called the "Manosphere" is a decentralized structure spread across different platforms. This network reproduces sexist stereotypes in popular and easily shareable forms, while the anonymity of perpetrators severely limits accountability.

- A study conducted in 31 countries reveals that young men think that advocating for gender equality constitutes discrimination against men.[6]

- Another study conducted in 2022 found a 59 per cent increase in violent rhetoric compared to the previous year, as well as a rise in content encouraging the sexual abuse of children.[7]

END DIGITAL VIOLENCE FULL STOP!



Who is subjected to digital violence?

Everyone!
However, because digital violence stems from the same structural inequalities and discrimination as gender-based violence, the violence experienced by women and girls is different and more frequent.

- Although globally comparable data are limited, the prevalence of violence against women in digital environments ranges between **16 per cent and 58 per cent**.[8]

- According to UN Women's November 2023 report "The Dark Side of Digitalization: Technology-Facilitated Violence Against Women in Eastern Europe and Central Asia", the average rate of women subjected to technology-facilitated violence across the 12 countries included in the study is **53.2 per cent**. In Türkiye, this rate is **72.4 per cent**[9]

- According to the findings of the study "Digital Violence in Türkiye", supported by UNFPA and published in 2021 by the Association for Social Information and Communication, **51 per cent** of women receive written, audio or visual harassment messages in digital environments, and **46 per cent** are subjected to cyber stalking.[10]

Who is at greater risk?

Women subjected to intimate partner violence are the highest risk group, but some groups are also disproportionately targeted in digital environments.[11]

Women leaders:

Women who are more visible in digital spaces are more likely to be subjected to digital violence. Women who are politicians, journalists, artists, writers, academics, athletes, and activists can, at times, become direct targets of perpetrators of digital violence.

- According to UNESCO research, **73 per cent** of women journalists have been subjected to online violence.[12]

- According to data from the Inter-Parliamentary Union, **81.8 per cent** of women politicians have been subjected to online harassment, and **44.4 per cent** have received threats of sexual or physical violence.[13]

Young women and girls:

Young people are much more active digitally, and this increases their risk of being subjected to digital violence.

- **58 per cent** of young women and girls aged 15-25 have experienced online harassment. **85 per cent** have been subjected to more than one form of digital violence.[15]

Women and girls with intersecting identities:

Women and girls can be subjected to digital violence in different ways and to disproportionate degrees due to intersecting characteristics such as age, occupation, education, disability, race or ethnic origin, migration status, gender identity and social position.

*"Particularly the violence perpetrated through social media increases in direct proportion to **women politicians' positions and power;** the violence directed especially at more visible women politicians can be discouraging for other women's participation in politics. **In this sense, the violence faced by one woman politician can indirectly create a barrier to another woman's participation in politics.**"*
(Violence Against Women in Politics in Türkiye – UN Women, 2023)[14]

Who perpetrates digital violence?

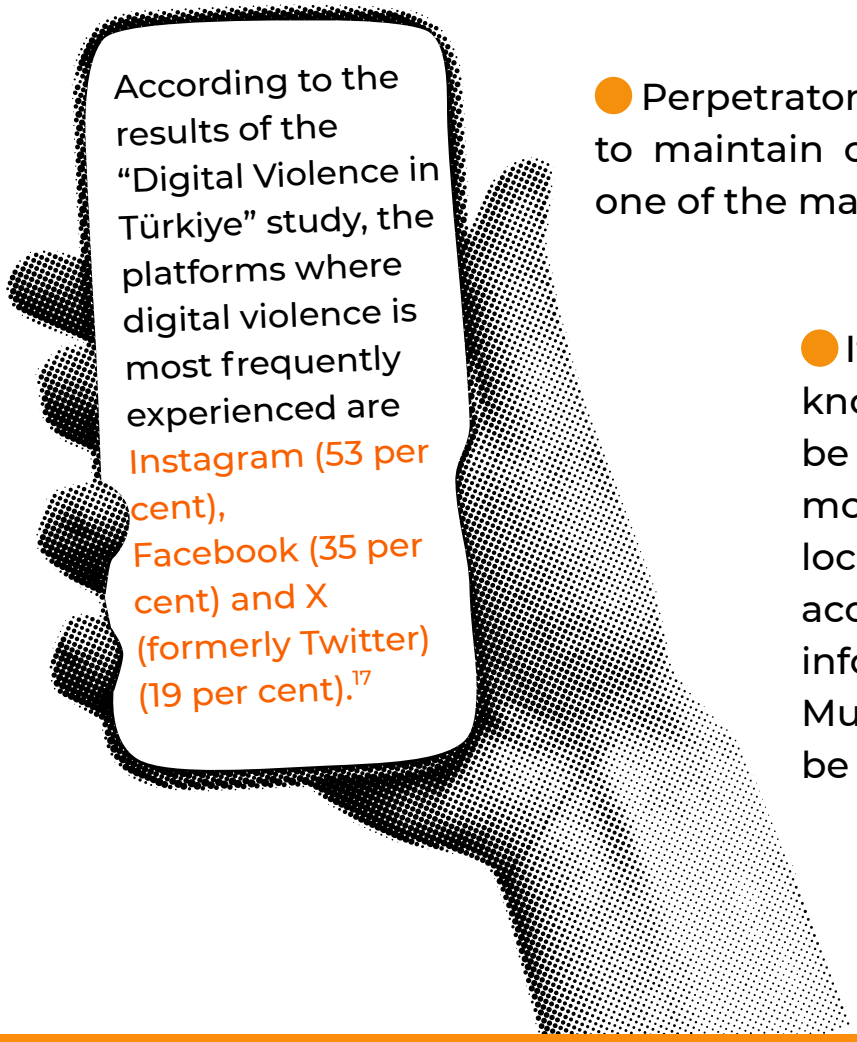
The person who commits digital violence may be a former or current spouse/partner, a neighbour, a colleague or classmate, someone close to you, or a stranger.

The majority of digital violence is perpetrated by unknown persons (50.3 per cent) or by people known only online (17.5 per cent). However, nearly one-third (32.1 per cent) of technology-facilitated violence is committed by people within women's social circles — such as partners, family members, friends, acquaintances, colleagues, supervisors or classmates — and is therefore an extension of offline violence.[16]

Even if perpetrators use different tactics and tools, their goal does not change: **to shame, humiliate, intimidate, threaten, silence, or encourage mob attacks and malicious advances.** All of these acts are part of the same mechanism of power and control that targets a person's safety and freedom of expression..

Where and how does digital violence occur?

Acts of digital violence are carried out through the use of Information and Communication Technologies (ICTs) such as social media and messaging platforms, apps, game chat rooms, forums and e-mail.



According to the results of the "Digital Violence in Türkiye" study, the platforms where digital violence is most frequently experienced are Instagram (53 per cent), Facebook (35 per cent) and X (formerly Twitter) (19 per cent).[17]

- Perpetrators are usually very determined to maintain control, and technology is just one of the many tools they use to do so.

- If you feel that the perpetrator knows a lot about you, they may be obtaining this information by monitoring your devices or location, accessing your online accounts, or gathering information about you online. Multiple ways and methods can be used to achieve this.

If you'd like let's reinforce this topic a bit with some examples...

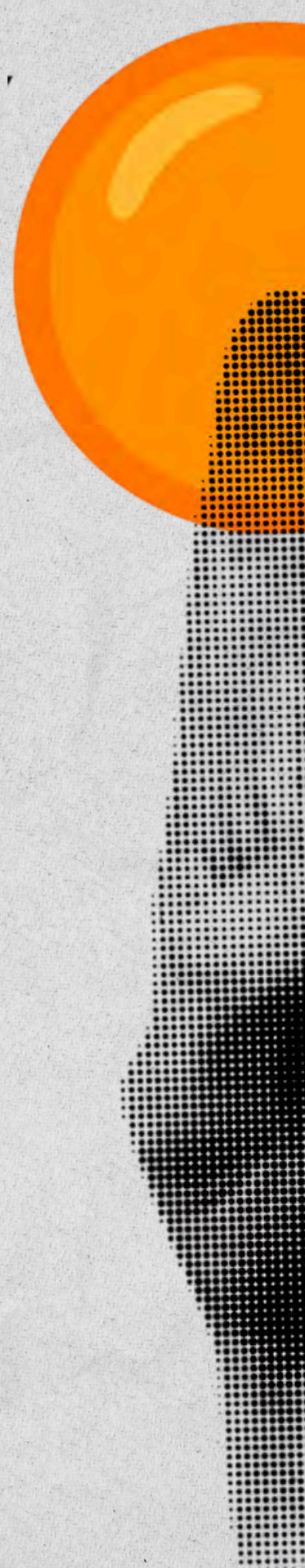
Types of digital violence are constantly changing as technology advances!

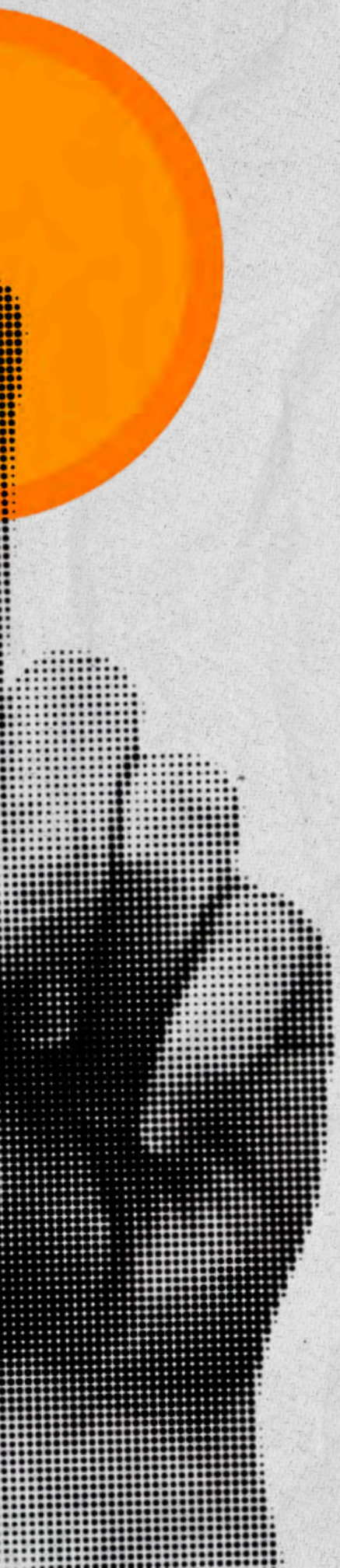
What are the most common types?[18]

- ONLINE SEXUAL HARASSMENT
- CYBERSTALKING
- IMAGE-BASED SEXUAL HARASSMENT (IMAGE-BASED ABUSE
- GENDER-BASED HATE SPEECH

What are the other concepts?

Astroturfing,
Catfishing,
Cross-Platform Harassment,
Cyberflashing,
Deadnaming,
Digital Voyeurism,
Doxing,
Electronically Enabled Financial Abuse, **Flaming**,
Gender-Trolling,
Gendered Disinformation,
Googlebombing,
Grooming,





Hashtag Poisoning, **Internet of Things (IoT) Abuse**, **Online Defamation**, **Online Impersonation**, **Malicious Distribution**, **Malware Attacks**, **Mass Reporting**, **Sealioning**, **Sextortion**, **Shadow Banning**, **Swatting**, **The Manosphere**, **Zoombombing**

Now let’s list these in the form of concept cards*:

*The Turkish equivalents of these concepts emerged in November 2025, as a result of a workshop convened by UN Women and UNFPA with nearly 30 representatives from civil society organizations and experts. The aim was to examine concepts and types of digital violence in depth from different perspectives and to develop a shared glossary of concepts in the field of digital violence.

Let’s start with the most common forms:

Online Sexual Harassment

WHAT IS ONLINE SEXUAL HARASSMENT?

A form of harassment that can include unwanted sexual attention and sexual coercion. It is also defined as "any unwanted sexual conduct conducted through digital means."[19]

Common methods / tools :

- Threatening physical or sexual violence in digital environments, making sexist jokes, commenting on physical appearance or sexual experiences, sending sexually suggestive messages, sending inappropriate sexual gestures, repeatedly asking a person for a date, making derogatory comments about a person's gender identity.[20]

Examples:

- A female politician received thousands of rape or death threats in one day after announcing her women's rights campaign.
- Female actors receiving sexually explicit images through social media or messaging apps

Cyberstalking

WHAT IS CYBERSTALKING?

Targeting someone through repeated and unwanted actions carried out via digital platforms and tools.[21] It is often an extension of offline stalking.

Common methods / tools:

- Repetitive disruptive behaviors via messaging, social media platforms, e-mail and phone
- Tracking someone's activity through spyware, mobile navigation apps, map tools, or device hacking
- Monitoring via smart home devices (cameras, etc.)

Examples:

- An ex-partner or current partner installing spyware to monitor someone's phone and location
- Consistently monitoring someone online and then showing up in places where the person is, continuing the harassment in real life.

Image-based Abuse

WHAT IS IMAGE-BASED ABUSE?

The practice, manipulation, or sharing of intimate, private, or sexual images/videos without consent, usually online. It also includes threats to create or distribute such material. These images or videos may have been obtained with or without the person's consent.[22]

Common methods / tools:

- Using AI-based tools to produce or edit images, videos, or audio that make someone appear to do or say things they never did (deepfake*)
- Sharing secretly recorded content, stolen files, or images obtained after hacking someone's account

Examples:

- An ex-partner threatening to share intimate images that were originally sent with consent
- Circulating AI-generated sexual images of a singer online to damage their reputation

* Images, videos, or audio edited or generated using AI-based tools to make someone appear to do or say things they did not actually do or say.

Gender-based Hate Speech

WHAT IS GENDER-BASED HATE SPEECH?

Expressions that spread, encourage, promote, or justify hatred based on someone's gender identity.[23]

Common methods / tools:

- Producing and sharing content that portrays women as sexual objects
- Posting sexist or insulting comments
- Using body-shaming, gender-based derogatory stereotypes, and mocking behavior in online spaces.

Examples:

- Sexist and sexually violent comments not being removed / remaining in posts directed at a female politician
- Producing content containing hate speech towards female players at sports events

Let's look at the other concepts in order:

Astroturfing

WHAT IS ASTROTURFING?

The coordinated creation and spread of content, often using multiple fake accounts, to make it look like a grassroots movement even though it is actually produced by an individual, interest group, political actor, or organization. This can include abusive or manipulative material.[24]

Common methods / tools:

- Using fake or anonymous accounts to create posts, run hashtag campaigns, and write coordinated comments to create the impression of a “widespread public opinion”
- Sharing misleading campaign messages with specific hashtags and spreading the same narrative across different platforms
- Spreading the same narrative across social media, forums, and messaging channels at the same time.

Examples:

- Sharing coordinated misogynistic content against equality-focused campaigns (such as women’s rights initiatives) to create the false impression that “society is opposed.”
- Bot accounts copy and paste messages saying "you're exaggerating" to the #NotSecure tag

Catfishing

WHAT IS CATFISHING?

Deceiving someone online by creating a fake identity or account —often using another person's photos and life details and making the target believe they are in a real friendship or romantic relationship. The goal may include emotional manipulation to obtain money, gifts, intimate images, or to later carry out blackmail.[25]

Common methods / tools:

- Creating fake profile(s)
- Building emotional closeness very quickly
- Asking for money, gifts, or bank details; inventing fake emergencies to request payments or transfers
- Impersonating a real person or hacking their account and pretending to be them

Examples:

- A perpetrator who, using a fake identity on dating apps and presenting himself as a wealthy person, gains the trust of multiple women and, under the pretext of an "emergency", makes financial demands and economically exploits them.

Cross-platform harassment

WHAT IS CROSS-PLATFORM HARASSMENT?

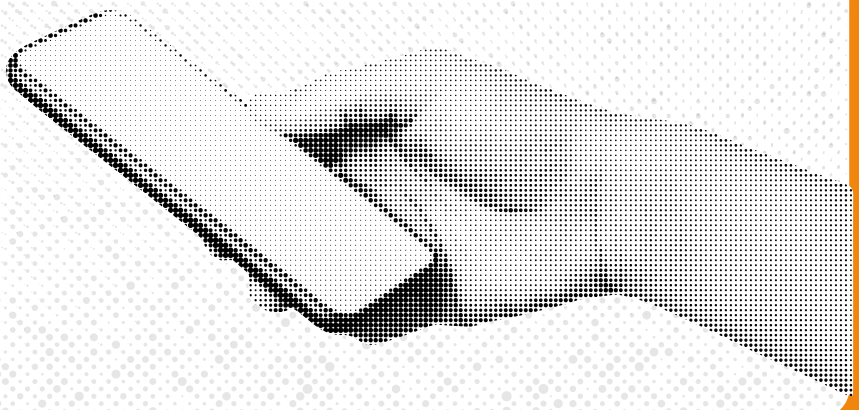
A perpetrator or group of perpetrators uses multiple social media and communication platforms simultaneously / consecutively and intentionally to harass a person/people.[26]

Common methods / tools:

- Launching attacks on the same target across different platforms at the same time (posting countless comments, sending messages, tagging)
- Creating the impression of "isolated incidents," since each platform only evaluates the harassment happening within its own system

Examples:

- A smear campaign started against a female journalist on X being carried over the same day to Instagram comments, YouTube video sections, and Telegram / WhatsApp groups in a coordinated way
- The creation of threads on Reddit targeting an activist's username, the production of manipulated videos on TikTok, and the multi-channel harassment and threats by users organized on Discord through Instagram messages and e-mails.



Cyberflashing

WHAT IS CYBERFLASHING?

Sending sexual images or videos without the recipient's consent through dating apps, messaging apps, e-mail, social media platforms, or file-sharing tools such as AirDrop. This act violates a person's privacy and is often considered a form of sexual harassment.[27]

Common methods / tools:

- Sending files via AirDrop or Bluetooth
- Sharing images through messaging apps, e-mail, or social media
- Showing sexual images during video calls or live streams

Examples:

- A person sending a sexually explicit photo, without consent, to a woman they have been communicating with via a dating app, violating her privacy making her feel unsafe in digital spaces.
- Sending unwanted sexually explicit images to nearby women via a file-sharing feature such as AirDrop while in public transport, in a café, or in another public space.

Deadnaming

WHAT IS DEADNAMING?

Intentionally revealing or using a person's former or birth name without their consent and against their preferences to cause harm. It refers especially to ignoring or maliciously spreading the old names of trans and non-binary people who have chosen new names.[28]

Common methods / tools:

- Ignoring the person's new name and tagging or captioning it with their old name on social media platforms, news sites or forums
- Using hashtag attacks or large volumes of repeated replies/comments to push the person's old name into circulation

Examples:

- A researcher requests that the name they no longer use be removed from their academic publications, but publishers ignore this request and the old name continues to circulate.
- A media outlet continues to use an artist's former name in news coverage, even though the artist is publicly living under their self-chosen name.

Digital Voyeurism

WHAT IS DIGITAL VOYEURISM?

Secretly capturing images or videos of individuals without their knowledge or consent. It can also be part of a longer pattern of stalking or exploitation.[29]

Common methods / tools:

- Taking non-consensual photos or videos with hidden cameras, smartphones, or devices disguised as pens, glasses, or remote controls
- Filming under someone's clothing or skirt (upskirting)
- Taking a non-consensual sexually suggestive photograph of a person without their consent (creepshot)

Examples:

- A hidden camera placed inside a store's fitting room recording customers while they are changing clothes
- Secretly filming in a school locker room with a smartphone and sharing the footage in private messaging groups

Doxing

WHAT IS DOXING?

Doxing is the collection and online sharing of personally identifiable information without a person's consent. It involves publicly disclosing private, personal, and sensitive information, such as a person's home and e-mail addresses, phone numbers, workplace and family members' contact information, or photos of their children and the schools they attend.[30]

Common methods / tools:

- Publishing someone's home or work address, phone number, location details, or their children's school information without consent
- Sharing private e-mails, message logs, personal photos, or intimate details to damage someone's reputation or shame them
- De-anonymizing a person revealing the identity of someone who uses an alias or anonymous account by exposing their old or current posts

Examples:

- Sharing a female politician's child's photo and school name, followed by violent threats sent to her e-mail and phone
- Releasing private message archives and old photos of a female actor to run a "smear" campaign against her

Electronically Enabled Financial Abuse

WHAT IS ELECTRONICALLY ENABLED FINANCIAL ABUSE?

The use of the internet and other digital technologies to exert financial control over a woman who is experiencing intimate partner violence.[31]

Common methods / tools:

- Restricting access to joint or personal accounts through online banking or password resets; constantly monitoring account activity and spending
- Lowering card or payment limits without consent, blocking online shopping or bill payments, and controlling digital wallets or payment apps
- Taking out loans, opening subscriptions, or creating fake debts in the person's name without permission; damaging their credit score
- Stealing personal data and using it for financial transactions; intercepting two-factor authentication codes to make unauthorized payments

Examples:

- The perpetrator blocked the woman's online shopping and made every expenditure dependent on his permission
- The perpetrator applied for a loan online on behalf of his wife and put her in debt.

Flaming

WHAT IS FLAMING?

Posting direct insults, profanity, or aggressive language in online spaces. Unlike gender trolling, the goal is not to create disagreement but to use openly hostile and provocative language. It often happens on forums, social media, and anonymous platforms, where anonymity encourages abusive behavior.[32]

Common methods / tools:

- Sending direct insults or profanity in comments on social media or forums
- Using anonymous accounts or fake profiles to post aggressive messages
- Planning content that is provocative, threatening or insulting

Examples:

- An academic who posts about violence against women is targeted by anonymous accounts sending direct insults, abuse and threats, forcing her to delete her posts and reduce her online visibility.
- Women users who express political views on online discussion platforms are targeted by anonymous accounts with constant insults, derogatory language and threatening messages, in an attempt to block their participation in debates, and many are forced to withdraw due to safety concerns.

Gender Trolling

WHAT IS GENDER TROLLING?

Gender trolling is a form of online harassment aimed at targeting, intimidating, or discrediting women, simply for being women when they express opinions on gender equality or other controversial topics. Although it is often presented as a "joke" or "mild criticism," it is rooted in gender-based hostility, condescension, and displays of power.[33]

Common methods / tools:

- Posting humiliating comments, insults, or defamatory content
- Coordinated troll attacks
- Direct threats and harassment

Examples:

- Women journalists, especially when they share reports on politics, women's rights or gender equality, are subjected to mass, organized troll attacks.
- A feminist media critic who challenges the representation of women in gaming culture is subjected to intense abuse, smearing and threats from organized troll groups after publishing her work, and is pressured into withdrawing from digital spaces.

Gendered Disinformation

WHAT IS GENDERED DISINFORMATION?

The use of false or misleading gender-based narratives often carried out with some level of coordination to undermine women, especially women leaders, discourage their participation in public life, and promote certain political or social agendas.[34]

Common methods / tools:

- Systematically spreading sexist stereotypes such as "incompetence," "emotional instability," or "immorality
- Combining gender-based attacks with misleading narratives about race, ethnicity, disability, or other identities

Examples:

- Circulating coordinated fake news and manipulated images to portray a female politician as "emotional" or "unfit"
- Turning fabricated claims about a female journalist's or activist's private life into a trending topic through bot networks, while simultaneously flooding her with threatening comments.

Google Bombing

WHAT IS GOOGLE BOMBING?

Manipulation of search engine results with the aim of damaging the online reputation of a person or institution. This method works by giving a large number of links (backlinks) to certain websites, causing that page to be associated with irrelevant or negative search terms and to appear at the top of search results.[35]

Common methods / tools:

- Creating a network of links in a way that manipulates search engine algorithms
- Associating negative content with the target's name
- Sharing links in a coordinated way through communities or bot accounts

Examples:

- In a search engine's autocomplete function, when a search is made about a politician's spouse, sexually explicit terms appear alongside her name.

Grooming

WHAT IS GROOMING?

The use of digital tools with the aim of luring a child into sexual abuse or child trafficking.[36]

Common methods / tools:

- Communicating through games, direct messages, comments, closed groups, concealing age / identity
- Isolating the child from family / friends, demanding to talk alone and in secret
- Requesting intimate images / videos, threatening to share them without consent

Examples:

- A perpetrator meets a 13-year-old user in a game and has "secret" conversations for weeks via direct messages, then asks for intimate images and threatens the user with "If you tell anyone, you'll get in trouble".
- An adult who pretends to be a "peer" on social media moves the child / teen off the platform (to an encrypted messaging app) and, using gifts / promises, asks them to send images.

Hashtag Poisoning

WHAT IS HASHTAG POISONING?

Flooding the content under a hashtag that was created to support women's rights and to open space for sharing experiences with messages that express the exact opposite.[37]

Common methods / tools:

- Finding hashtags that create space for women and are used to amplify their voices
- Posting enough content under those hashtags to dominate them

Examples:

- Feminist hashtags like #TakeBackTheTech and #ImagineaFeministInternet were flooded with coordinated misogynistic messages and digital images meant to "wipe out" these campaigns.
- The #YesAllWomen hashtag, created for women to share their experiences with gender-based violence, was taken over by some male users who added dismissive, mocking, or sexist comments that minimized women's stories.

Internet of Things (IoT) Abuse

WHAT IS INTERNET OF THINGS (IOT) ABUSE?

The act of the perpetrator using smart home devices, wearable technologies and connected household appliances to gain control over a person. It is carried out in order to monitor, manipulate and place psychological pressure on the person's daily life.[38]

Common methods / tools:

- Controlling the home's temperature via smart thermostats
- Monitoring a person's daily activities through smart devices
- Listening in on conversations via voice assistants and other connected devices

Examples:

- An ex-husband gaining access to the health data of a woman who uses a wearable health-tracking device, and obtaining information about her health status without her consent.
- An ex-husband accessing the smart home system without permission and listening to the woman's conversations through the iPad in the house.

Online Defamation

WHAT IS ONLINE DEFAMATION?

The spread of false or distorted information about a person or entity over the internet, thereby damaging their reputation. It generally aims to humiliate, threaten, discredit, intimidate or punish a person / entity. Women who are more visible in public life, such as politicians, journalists, activists, and artists, are most often targeted.[39]

Common methods / tools:

- Sharing deliberately produced false or distorted information on social media platforms
- Conducting smear campaigns using altered images, videos or documents
- Making false / baseless content “trend topics” (TT) to reach wider audiences through multiple posts using hashtags

Examples:

- A coordinated smear campaign against a journalist on social media, where dozens of accounts share the same false information at the same time
- Spreading manipulated visuals in order to discredit an activist

Online Impersonation

WHAT IS ONLINE IMPERSONATION?

Creating a fake social media account in order to defame a person, discredit them, or trigger further abuse. It also includes misrepresenting someone and creating content in their name without their consent.[40]

Common methods / tools:

- Creating social media accounts using someone else's identity
- Using artificial intelligence to create deepfake videos or images
- Sharing content that damages the person's identity and reputation

Examples:

- A man creating a detailed profile in a sexual content website under a woman's name, using her personal information.
- During election periods, fake accounts being created under the names of women politicians, spreading statements that do not match their campaigns.

Malicious Distribution

WHAT IS MALICIOUS DISTRIBUTION?

The use of technology-based tools to distribute material that damages the reputation of individuals and / or organizations, such as their intimate photos / videos.[41]

Common methods / tools:

- Malicious distribution of someone's data without their consent
- Seizing data held by women's support mechanisms
- Sharing personal information through social media platforms

Examples:

- In a private Facebook group made up of male members, the men shared nude photos of their wives and girlfriends without their consent.
- Personal data held by a clinic providing abortion services is distributed in order to incite violence against the women who have used the service.

Malware Attacks

WHAT ARE MALWARE ATTACKS?

The sending / transmission of malicious software to a device when the user clicks on a link in an e-mail or message that contains malware, opens an attachment, or visits a website. Content containing such malicious software often appears to come from an official e-mail address, an acquaintance or a colleague.[42]

Common methods / tools:

- Statements/bills sent as e-mail attachments
- Discount messages shared via chat applications
- Malicious software embedded into websites

Examples:

- During the election period when she was running as a candidate, malicious software was placed on a woman politician's website, leading to visitors' devices becoming infected with a virus.
- A woman received an e-mail saying that her friend had shared the photos taken last summer, and when she clicked the link, the information on her computer was accessed and stolen.

Mass Reporting

WHAT IS MASS REPORTING?

A practice that occurs mostly on Instagram but also on X (formerly Twitter), where an account or a content is reported systematically and en masse. Reporting is generally carried out by a particular group to prevent the user's voice from reaching a wider audience, and there is no meaningful / valid reason for being reported.[43]

Common methods / tools:

- Complaint/report mechanisms on platforms
- Organized trolls

Examples:

- Coordinated trolls sharing an account or a piece of content among themselves and using reporting mechanisms to file complaints at the same time.

Sealioning

WHAT IS SEALIONING?

Persistently questioning someone, often about basic, easily available information or irrelevant points, in order to wear them down or provoke them, and forcing them to respond. The motivation is to drain the other person's energy and patience, strain their nerves, and to try to produce material (screenshots) from go-nowhere debates that can be shared later.[44]

Common methods / tools:

- Luring someone into endless, pointless debates on public social media platforms.

Examples:

- When a woman journalist shares content on X about gender equality, some users ask questions that seem harmless, such as "But what exactly do you mean?", "Which country are you talking about when you say women don't have equal rights?", or "Can you show me the statistics?", creating an endless loop
- When a feminist media critic shares content about harassment, she is exposed to hundreds of supposedly "reasonable" questions such as "Do you really have proof?", "I'm just curious, why are you saying that men aren't harassed?", or "Can you explain exactly what being a feminist means?"

Sextortion

WHAT IS SEXTORTION?

When a person has, or claims to have, a sexual image of someone else and uses it to force that person to do something they do not want to do.[45]

Common methods / tools:

- A perpetrator threatening to distribute images that were previously shared with consent, or obtained through hacking / fraud
- Threatening the victim by claiming to have deepfake or manipulated images
- Threatening with claims such as “I hacked your computer / camera and took nude photos of you”
- An ex or current partner using previously shared images as a tool of threat

Examples:

- A perpetrator claims to have hacked a person’s computer and obtained nude images, and demands money.
- During a divorce, an ex-husband uses the sexual images he has of his ex-wife as a threat, saying “I’ll send them to your family” in order to prevent the divorce.

Shadow Banning

WHAT IS SHADOW BANNING?

A practice that occurs mostly on Instagram but also on X (formerly Twitter), where, as a result of systematic and mass reporting of your account or one of your posts, your content can only be seen by your followers or by a limited portion of them. It is not very likely that users subjected to this will realize it directly; a marked drop in engagement numbers is one indication.[46]

Common methods / tools:

- Complaint / report mechanisms on platforms
- Coordinated trolls

Examples:

- As coordinated trolls share an account or a piece of content among themselves and use reporting mechanisms to file complaints at the same time so that the user's posts end up not reaching a large part of their followers.

Swatting

WHAT IS SWATTING?

The act of making a fake phone call or online report to law enforcement, claiming that an incident requiring police intervention is taking place at the target's home or workplace, thereby causing a fully armed police unit to be dispatched to the target's address.[47] Its name comes from the U.S. police unit "SWAT" (Special Weapons and Tactics), which uses militarized techniques, equipment and firearms.[47]

Common methods / tools:

- Phone calls
- Online reporting methods

Örnekler:

- After a phone tip claiming that a murder had taken place in her home, the house of a well-known actress was raided.
- By using online reporting methods, an influencer was woken up in the early morning when nearly 30 armed police officers raided her home.

The Manosphere

WHAT IS THE MANOSPHERE?

Online male community networks that claim to defend various "men's rights" and interests while promoting misogynistic ideologies and anti-feminist, sexist beliefs.[48]

Sub-groups:[49]

- **Involuntary celibates (incels):** Men who, because of their perceived inadequacies about having sex (their own view), make misogynistic accusations against women.
- **Men's Rights activists (MRas):** Men who, often in an academic tone, claim that feminism and women's rights —such as the right to vote, access to education and leadership positions— have disadvantaged men.
- **"Pick up artist"s (PUa's):** Men who mock the concept of sexual consent.
- **"Men Going Their Own Way" (MGTOW) movement:** Men who argue that society is built against men's interests and that it is best to stay away from women and even mainstream society as a whole.

Examples:

- Calls for violence against women increasing on online incel forums, and some individuals committing acts of violence influenced by these ideologies
- PUA content creators on social media platforms sharing videos that teach men to ignore women's "No," mocking the concept of consent
- In political debates, MRAs (men's rights activist groups) targeting women leaders and describing feminism as "social collapse"

DISCOURSES:

RED PILL IDEOLOGY / BEING "REDPILLED":

Means “waking up” to a supposed reality where women are favoured over men. Refers to the 1999 sci-fi action film The Matrix, implying that those who think otherwise have taken the blue pill.

AWALT: "ALL WOMEN ARE LIKE THAT":

Used to stereotype women.

"FEMOID" - "FHO"S (FEMALE HUMANOID ORGANISM):

A derogatory term implying that women are not only inferior to men but also less than human.

"HYPERGAMOUS":

A term used in a derogatory way to suggest that women are obsessed with “marrying up,” based on the belief that women prefer partners with higher status, wealth or better looks than themselves.

Zoombombing

WHAT IS ZOOMBOMBING?

Zoombombing is when unwanted and uninvited users or groups of users invade / crash an online meeting and disrupt it. This disruption happens when uninvited people, change their names to obscene words, or exploit gaps in the meeting permissions, without the host’s permission, to share video / audio containing sexist, offensive or hate speech content.[50] The term comes from the fact that during the COVID-19 pandemic many events moved to the meeting platform Zoom.[51]

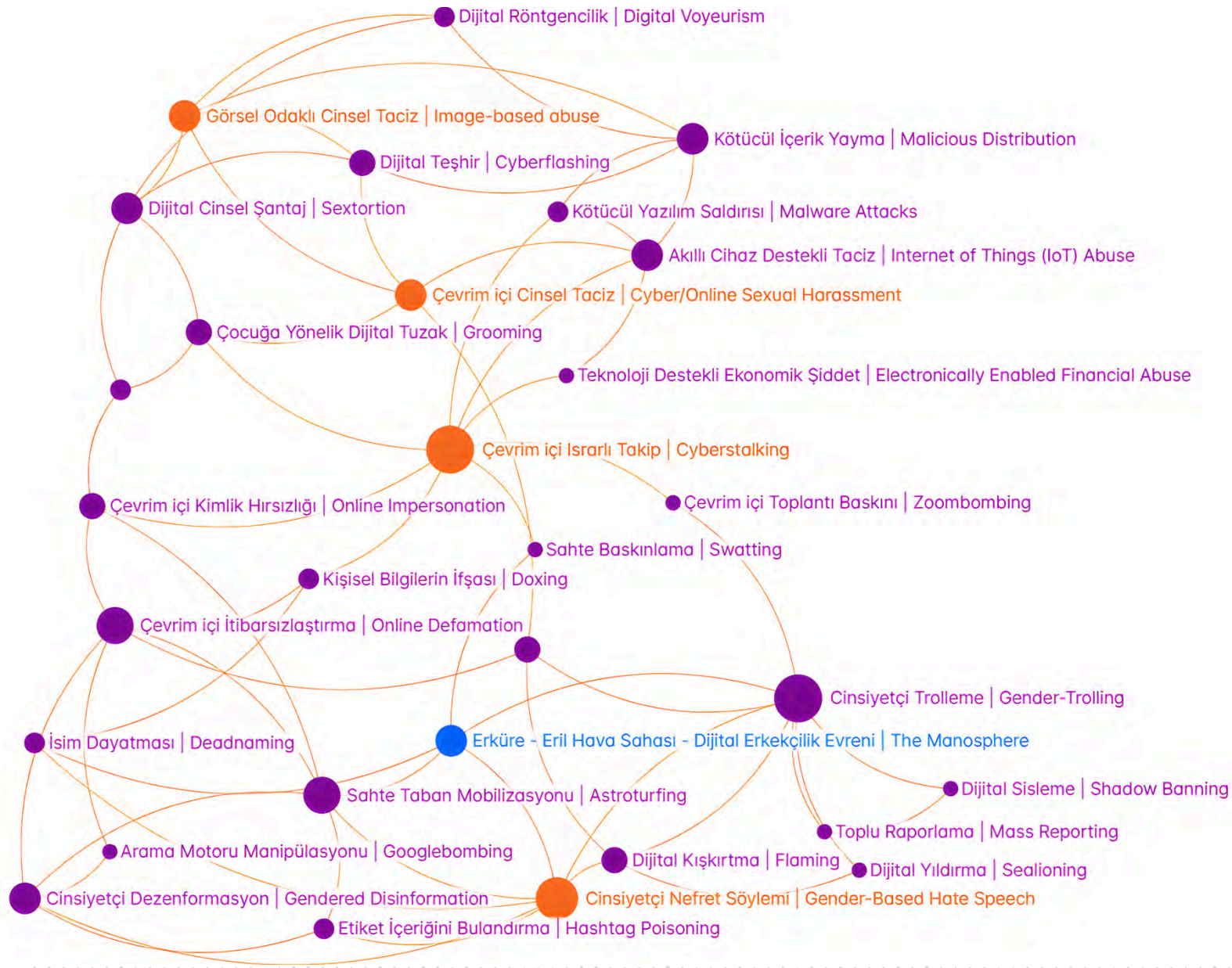
Common methods / tools:

- Sharing video and / or audio without permission
- Changing username
- Taking control of the meeting

Examples:

- At a university, a female professor organized an informal meeting to talk about sports, and shortly after the meeting began, 5–6 users entered the session and displayed explicit images, causing the professor to completely lose control of the meeting

All of these concepts are connected to one another!
To better understand how they relate,
click the link below or
scan the QR code!



The Effects of Digital Violence

Digital violence strengthens patriarchal roles, norms, and structures, making gender equality harder to achieve and creating a major barrier to reaching Sustainable Development Goal 5: achieving gender equality and empowering all women and girls.

When exposed to digital violence, we may feel anger, confusion, helplessness, fear, sadness, or worry about our own safety. We may also fear that our family or friends will find out.

We might minimize what happened to us, blame ourselves, or feel as if there is nothing we can do to change the situation.

Feeling confused or unsure about what to do next is completely normal.

It is also common and understandable for someone to keep their experience of violence to themselves for a while, especially due to safety concerns or uncertainty.

Those who experience digital violence often experience disruptions to their social and professional lives, limiting their mobility. Women can often experience fear, anxiety, and depression as a result of digital violence, which can lead them to close their social media accounts and withdraw from online spaces.

Closing a social media account may seem like a small action. But for women and girls, it often means stepping away from the digital world entirely. Digital violence aims to silence women online. It is also used to reduce their participation in public and political life, democratic processes, and leadership roles.

Everyone has the right to feel safe, free, and able to express themselves in public, private, and digital spaces.

How Can You Keep Yourself Safe?

Being targeted online can make you feel ashamed, unsafe, overwhelmed, or out of control. Sometimes you may not even want to take action. But without blaming yourself, there are steps you can take.

Here are a few:

- **Trust yourself.**
- You can start by trusting yourself and identifying what you are experiencing as violence.
- Remember: **It is not your fault!** Keep reminding yourself and others around you who are in similar situations that you shouldn't blame yourself and that there can be no justification for violence.
- Feelings, needs, and actions following an experience of violence can vary from person to person!

Talk to someone you trust or seek professional support....

- You can talk to a friend, a family member, or someone else you trust about what happened and how it made you feel.
- You know best who the people you trust are.
- You can seek counselling from specialists such as psychologists, lawyer or IT experts.
- You can also contact women's counselling centres.

Do Something That Makes You Feel Good!

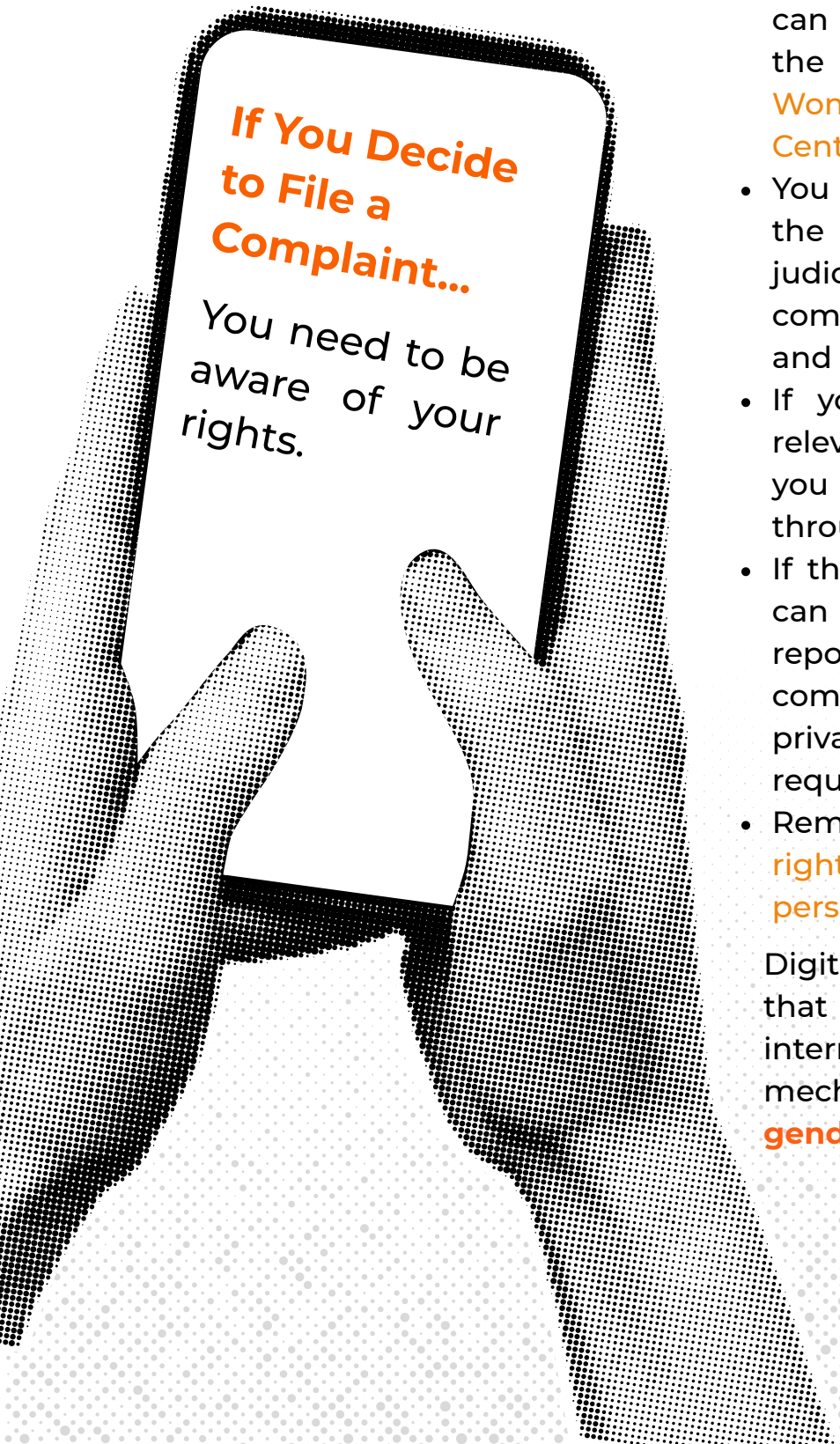
If being online feels challenging or exhausting at times, you can create a small space for yourself each day and take some distance from the digital world for a while.

Spend time doing things you enjoy on your own or with friends. Even reducing your screen time can be a good place to start.

Collect Evidence!

Begin by **documenting** the digital violence you have experienced. If you decide to pursue legal action, you will need this evidence. It can also help you understand your situation and plan for your safety.

Don't forget to take screenshots and back them **up in case** they get deleted or destroyed. You can also use the **E-Tespit system** provided by the Turkish Notaries Association to officially record the content you want to document. (https://e-hizmet.tnb.org.tr/tespit/)



- To learn about the legal process, you can consult with lawyers working on the issue and the Bar Associations' Women's Counseling Centers/Commissions.
- You can file a criminal complaint with the police or gendarmerie units or judicial authorities. Don't forget to compile all the relevant information and documents beforehand.
- If you decide to report it to the relevant institutions, ask someone you trust to accompany you throughout the process.
- If the perpetrator is a coworker, you can report it to your institution's reporting mechanism (ethics committee, etc.). Protecting your privacy is very important, and you can request this.
- Remember, it is your fundamental right to request the protection of your personal data and privacy.

Digital violence includes examples that constitute a crime. National and international legislation provides mechanisms you can use to **combat gender-based digital violence:**

International Agreements:

- Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW)
- Convention on Cybercrime (Budapest Convention)

National Legislation:

- Law No. 6284 on the Protection of the Family and the Prevention of Violence Against Women
- Law No. 5651 on Regulating Online Publications and Combating Crimes Committed Through These Publications
- Law on the Protection of Personal Data
- Turkish Penal Code

Online Reporting Channels:

- https://www.turkiye.gov.tr/btk-internet-ihbar-basvurusu
- https://ihbar.ng112.gov.tr
- Women's Support App (KADES)
- Vodafone App (Kırmızı Işık)
- UNFPA App(AMBER)

Institutions you can contact:

- Police Stations, Gendarmerie Stations
- Violence Prevention and Monitoring Center (ŞÖNİM)
- Judicial Authorities (Public Prosecutor's Office, Family Courts, and Legal Aid Centers)
- Women's Counseling Centers
- Bar Associations' Women's Counseling Centers

Emergency Phone Numbers You Can Call:

- **112** Emergency Call Center (Police, Gendarmerie, Medical Assistance)
- Alo **183** – 24/7 Violence Prevention Hotline (For people with hearing or speech impairments: +90 549 381 01 83)
- Domestic Violence Emergency Support Line +90 212 656 96 96 / +90 549 656 96 96
- **157** YIMER (for those who speak languages other than Turkish)

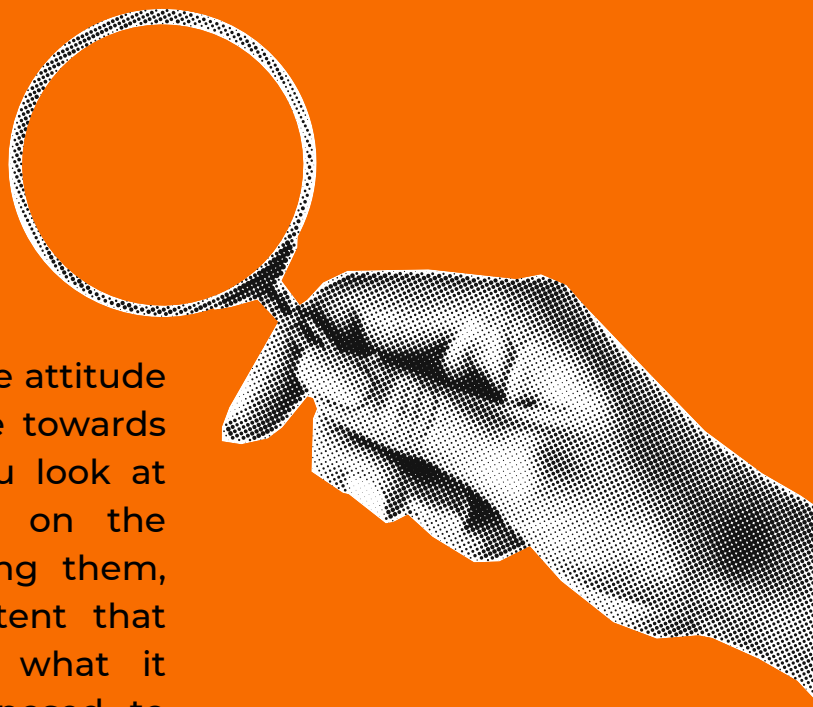
There are so many things you can do to strengthen your digital safety. Remember, the power is in your hands!

We are taking control in the digital world!

There are things you can do to keep yourself and all users safe on digital platforms.

It is possible to take a little time and try to make digital platforms safe for everyone!

DO YOU KNOW THE PLATFORM YOU'RE USING?



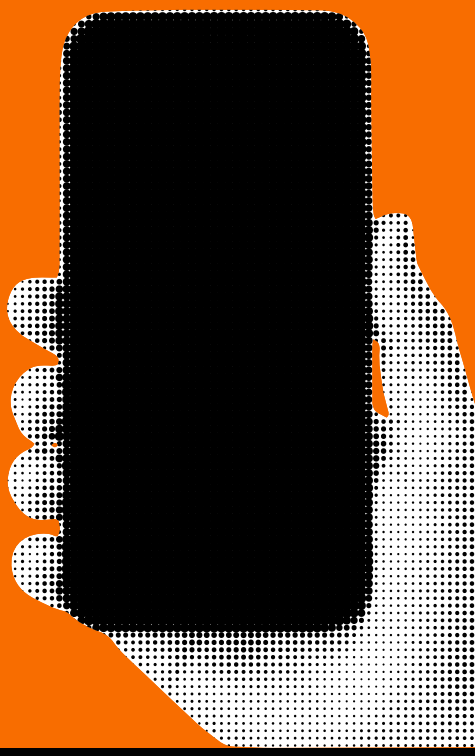
First, you need to be aware of the attitude of the digital platforms you use towards harassment and violence. If you look at the sections on these topics on the platforms before you start using them, you can find out to what extent that platform will protect you or what it promises to do if you are exposed to violence or harassment. You can then decide whether or not to use that platform.

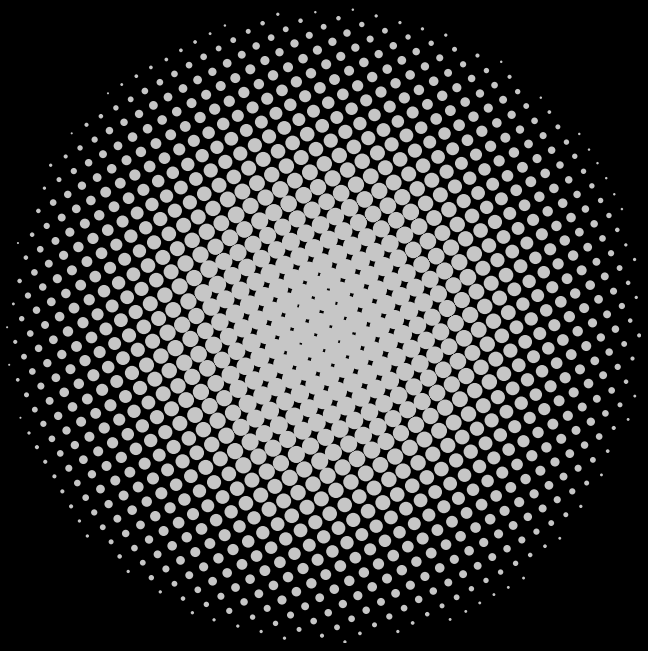
ARE YOUR PASSWORDS STRONG ENOUGH?

You should change your passwords regularly and avoid using very common ones such as "12345," "qwerty," or "qwerty123." These can be cracked in less than a second, making them a serious threat to your digital safety. Also remember to treat your password as personal data—never share it with anyone, even people you trust.

ARE YOU THE ONLY PERSON WHO KNOWS THE ANSWERS TO THE SECURITY QUESTIONS?

When you register, digital platforms ask you to set a security question and answer to help you if you forget your password. Make sure you are the only one who knows the answer to this security question. Be careful when talking to those around you about this, as you may inadvertently share the answer to this question. Also, be mindful of what you share on digital platforms, especially if the security question relates to your childhood (your first pet, the name of your elementary school, your favorite elementary school teacher, etc.), and in trends like #tbt (a trend where users share memories from the past with the #ThrowBackThursday tag).





MULTIPLE PLATFORMS, ONE PASSWORD?

Using the same password across all your digital platforms puts your security at risk.

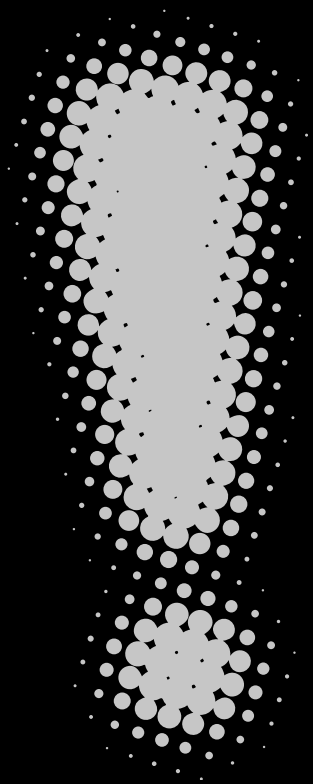
Using the same username–password combination everywhere is even more dangerous.

If one platform experiences a data breach and your login details are exposed, attackers can try the same combination on other platforms and gain access to your accounts.

HAVE YOU SET UP YOUR SECURITY SETTINGS?

On digital platforms, you should go to the security and privacy sections right from the start and configure the settings you deem necessary. Choosing who can see the e-mail address or phone number you used when signing up, deciding who can see your content, determining which words will be filtered in comments, and setting up which behaviors of your followers you can restrict are just a few examples.

For example, using Instagram's limited interactions feature, which allows you to temporarily restrict unwanted comments and messages, can make you feel safer.



DID YOU ENABLE TWO-FACTOR AUTHENTICATION?

Most digital platforms offer two-factor authentication. This feature sends you a code or notification via your preferred verification method when you attempt to log in from a different device. You will not be allowed to log in without completing this verification. This allows you to securely access your account when switching devices or browsers.

HAVE YOU ALLOWED THIRD-PARTY APPLICATIONS?

Sometimes, when joining a new platform, logging in with your Google, Facebook, or another existing account seems faster than creating a new profile. But this also means the new platform may gain access to certain data stored in your existing accounts, which can create security risks. You can revoke this access later through your security settings. For example, in the security section of your Google account, under “Third-party apps and services,” you can view which apps you've granted access to and remove any apps you don't remember or recognize.

DO YOU USE REPORTING TOOLS?

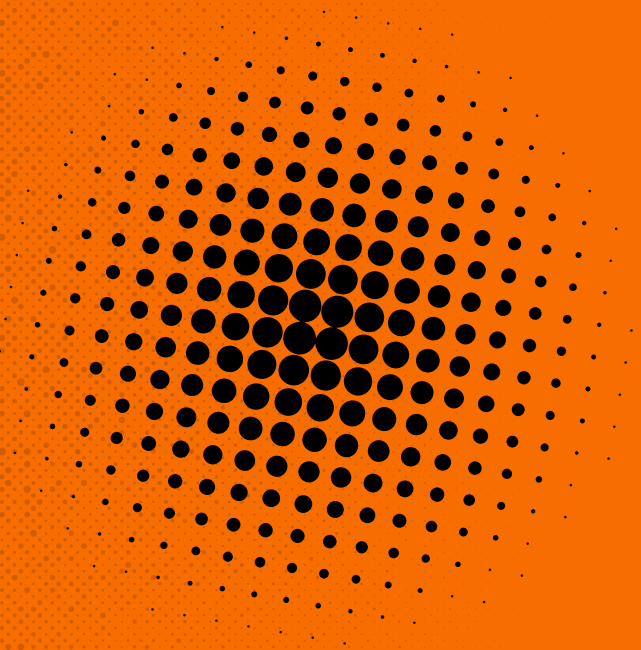
If you experience digital violence, you should use the reporting system of the platform where the incident occurred. By doing so, you help make the platform safer not only for yourself but for all users.

When using reporting tools, make sure you choose the correct category so your report can be evaluated properly. Also remember that you can report a profile, a piece of content, a video thumbnail, or an entire video separately. Reporting options may vary from platform to platform and can change over time, so it’s helpful to review the reporting categories periodically.

DO YOU PAY ATTENTION TO YOUR SECURITY İN SHARED SPACES?

It is safer to use your own internet connection instead of the ones provided in shared spaces or accessible by people you don’t know. You can even use your phone as a modem when you need an internet connection for your computer.

Also, when using a computer in a shared space, remember to log out of all platforms you've logged into and clear your browser history.



DO YOU SHARE YOUR LOCATION INFORMATION?

When you feel vulnerable to digital violence (such as a stalking partner), it is beneficial not to share your real-time location. You should keep yourself safe by avoiding actions such as checking in at a location or adding location information to a photo you uploaded before leaving that location.

IS THERE AN APP ON YOUR DEVICE THAT YOU DON'T RECOGNIZE?

You should regularly check your phone, computer, or tablet for apps that you didn't install. If you encounter an unfamiliar app, you should remove it. These apps may have been installed on your devices by others to track you.

This is especially important for detecting keyloggers, which record every keystroke on your device. Such spyware is most often found on devices received as gifts or those recently returned from service..

Some apps may be system apps, so if you see something unfamiliar, it’s best to look it up before deleting it.

WHEN YOU NEED TO TAKE YOUR PHONE IN FOR SERVICE...

Some Android phones have a “Maintenance mode” feature under “Battery and Device Care” or “Quick Services” in the “Settings” section. If you activate maintenance mode, only basic apps will be visible on the phone, and none of your personal information will be accessible. You will need your phone's passcode to exit Maintenance Mode. This feature ensures that the technical team cannot view any of your private information when your phone is sent for service.

Before taking your iPhone or iPad for repair, make sure to back up your device, turn off Apple Cash, remove your cards and transit passes from Apple Wallet, and disable Find My.

DID YOU LOG OUT OF ALL YOUR ACCOUNTS BEFORE CHANGING DEVICES?

When switching to a new phone, tablet, or computer, make sure you log out of all your accounts before resetting your old device to factory settings. You can also check the security settings of the digital platforms you use to see which devices your account is currently logged in on.

You may not be able to view every section of your apps' security settings on your mobile device. The safest approach is to log in to the relevant platform via a browser on your computer and check the security settings there.

ARE YOU SURE YOU DIDN'T GET PHISHED?

Not every e-mail you receive has good intentions. Sometimes clicking a link or opening an attachment can activate malicious software intended to collect your data or track your activity. These harmful programs may be hidden in what looks like a PDF bill from a phone operator you don't use, or in a link supposedly sent by a friend to show you their holiday photos. To test how familiar you are with phishing attempts, you can try: https://phishingquiz.withgoogle.com

There are things you can do for others too!

- You can report digital violence experienced by others to the relevant social media platform.

- You can send a message of support to someone whether you know them or not, to show that they are not alone.

- The perpetrator may even be someone you know. If you catch yourself making excuses for them, question those thoughts and remember that violence has no justification.

- Avoid liking, sharing, or amplifying hateful or sexist content.

- Always ask for permission before tagging someone in a post. You can never know what kind of safety risk a simple tag might create for them.

And of course, you can start by sharing this guide...

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.

[2]UNGA 79: Intensıfıcatıon of Efforts to Eliminate All Forms of Violence
Against Women and Girls: Technology Facilitated Violence Against Women and Girls Report of the UN Secretary General (2024)

[3]UNFPA (2021). Technology-facilitated Gender-based Violence: Making All Spaces Safe.

[4] UNGA 79: Intensıfıcatıon of Efforts to Eliminate All Forms of Violence
Against Women and Girls: Technology Facilitated Violence Against Women and Girls Report of the UN Secretary General (2024)

[5] Sensity AI. (2019). The state of deepfakes: A deepfake landscape and threat report.

[6] IPSOS (2024). International Women's Day 2024: Global Attitudes Towards Women's Leadership.

[7] Center for Countering Digital Hate (2022) The Incelosphere: Exposing pathways into incel communities and the harms they pose to women and children.

[8] UNGA 79: Intensıfıcatıon of Efforts to Eliminate All Forms of Violence
Against Women and Girls: Technology Facilitated Violence Against Women and Girls Report of the UN Secretary General (2024)

[9] UN Women (2023). The dark side of digitalization: Technology-facilitated violence against women in Eastern Europe and Central Asia.

[10] TBİD (2021). Türkiye'de Dijital Şiddet Araştırması.

[11] Bu bölüm, Dunn (2020) ve UNFPA (2021) raporlarından derlenmiştir.
Dunn, S. (2020). Supporting a Safer Internet Paper No. 1: Technology-Facilitated Gender-Based Violence: An Overview. Centre for International Governance Innovation (CIGI).
UNFPA (2021). Technology-Facilitated Gender-Based Violence: Making All Spaces Safe.

[12] UNESCO (2021). The chilling: global trends in online violence against women journalists

[13] Inter-Parliamentary Union (2016). Sexism, harassment and violence against women parliamentarians

[14] Un Women (2023). Türkiye'de Siyasette Kadınlara Yönelik Şiddet.

[15] Plan International (2020). Free to Be Online? Girls' and young women's experiences of online harassment

[16]16 UN Women (2023). The dark side of digitalization: Technology-facilitated violence against women in Eastern Europe and Central Asia.

[17]TBİD (2021). Türkiye'de Dijital Şiddet Araştırması.

[18] EWL (2024). Report on Cyber Violence Against Women.

Concept Cards References:

[19] UNFPA(2021). Technology-facilitated Gender-based Violence: Making All Spaces Safe.

[20] UN Women. How to address online sexual harassment during COVID-19.

[21] https://tfgbv.humane-intelligence.org/abuse-type/cyberstalking.

[22] European Women's Lobby (2024). Report on Cyber Violence Against Women.

[23] European Parlement(2018). Cyber violence and hate speech online against women.

[24] Pen America. Defining "Online Abuse": A Glossary of Terms.

[25] European Women's Lobby (2024). Report on Cyber Violence Against Women.

[26] WMC. Online Abuse 101.

[27] WomensLaw (2024). Abuse Using Technology.

[28] https://womensmediacenter.com/speech-project/online-abuse-101

[29] https://tfgbv.humane-intelligence.org/abuse-type/voyeuristic-recording/

[30]https://tfgbv.humane-intelligence.org/abuse-type/doxxing.

[31] https://womensmediacenter.com/speech-project/online-abuse-101.

[32] https://techterms.com/definition/flaming.

[33] UNFPA (2024). Digital Duality: How the Internet Empowers and Endangers Women

[34] Foreign, Commonwealth & Development Office (2023). Technology-facilitated gender-based violence: preliminary landscape analysis.

[35] European Women's Lobby (2024). Report on Cyber Violence Against Women.

[36] UNFPA(2021). Technology-facilitated Gender-based Violence: Making All Spaces Safe.

[37] Pen America. Defining "Online Abuse": A Glossary of Terms.

[38] https://tfgbv.humane-intelligence.org/abuse-type/iot-abuse.

[39] WMC. Online Abuse 101.

[40] https://tfgbv.humane-intelligence.org/abuse-type/online-impersonation.

[41] European Women's Lobby (2024). Report on Cyber Violence Against Women.

[42] European Womens' Lobby #HerNetHerRights Guide

[43] https://onlinelibrary.wiley.com/doi/abs/10.1002/poi3.359

[44] https://womenlobby.org/new-publication-report-on-cyber-violence-against-women/

[45] Suzie Dunn, "Technology-facilitated gender-based violence: an overview", https://apo.org.au/node/309987

[46] https://en.wikipedia.org/wiki/Shadow_banning

[47] https://onlineharassmentfieldmanual.pen.org/defining-online-harassment-a-glossary-of-terms/

[48] https://womenlobby.org/new-publication-report-on-cyber-violence-against-women/

[49] https://www.unwomen.org/en/articles/explainer/what-is-the-manosphere-and-why-should-we-care

[50] https://onlineharassmentfieldmanual.pen.org/defining-online-harassment-a-glossary-of-terms/

[51] https://apo.org.au/node/309987

UNFPA

turkiye.unfpa.org
infoturkiye@unfpa.org

UN WOMEN

turkiye.unwomen.org
infoturkiye@unwomen.org

@unwomenturkiye
@unfpaturkiye