Safe online

Digital technology is a fundamental part of our lives: it is everywhere and we use it constantly. It is important to know how we can increase our online security so that we continue browsing **feeling free and safe.**

95% of online abuse occurs against women, mostly by partners or exes

58% of teenage girls and young women experience harassment on social media almost daily

70% of women who experience cyberviolence also experience physical or sexual violence[1]

71% of perpetrators of violence within a relationship check partners' devices

If you think it's normal. Or if you have the feeling that it is not but you would not be able to say why.

If you think it won't happen to you. Or if you feel that maybe you might be at risk but you don't know how.

If you want to know more because, it's true, we live connected. Or if you find yourself in difficulty, for yourself or for your friend, sister, colleague, neighbor, mother, daughter.

This handbook is useful for:

- Knowing **how to protect yourself**
- Being able to **help** other women close to you
- Making you **think**, even if everything is fine

Forms of digital violence against women

The **digital dimension of violence against women**[2] includes both abuses that occur online and those that are facilitated by technology, and there is continuity between online and offline. The medium is virtual, but the abuse is real and its effects are concrete.

Cyberviolence against women and girls[3] includes many forms of cyber-based violence on gender related grounds.

Acts of cyberviolence against women and girls can

- start online and continue offline, in physical locations, such as at work, school or home;
- start offline and continue online via different platforms, such as social media, email or messaging apps;
- be acted upon by a person (or group of persons), anonymous or unknown to the woman;
- be acted upon by a person (or group of people) that the woman knows, such as a (former) partner, classmate or colleague.

Blanquerna Universitat Ramon Llull · kaspersky · UNA CASA PER L'UOMO società cooperativa sociale · www.work-with-perpetrators.eu · Regione del Veneto

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

Forms of digital violence against women

RESTRICTING DIGITAL ACCESS

Prevent or limit the use of devices such as phone, PC or tablet, apps or internet connection, with the aim of controlling or isolating a person, or threatening to do so, with the aim of manipulating him.

CYBERSTALKING AND CYBERSURVEILLANCE

Use of computer tools to harass, intimidate, spy on a person, making them feel threatened and insecure.

This can be done by logging into devices and accounts via

- Device usage request
- Using shared or stolen passwords
- Access to shared or unsecured devices
- Installing spy apps (stalkerware)
- and/or through the use of devices such as
- Car GPS or tracking devices
- Video surveillance systems
- Smart home devices (e.g. Google home or Alexa)

CYBERHARASSMENT AND CYBERBULLYING AGAINST WOMEN AND GIRLS

Harassment through emails and messages, online profiles and internet pages, with the purpose or effect of creating an intimidating, hostile, degrading, humiliating or offensive environment for the victim.

These are:

- Unsolicited email or message
- Offensive or inappropriate requests on social media or chat rooms
- Threats of physical or sexual violence via email, messages or chat
- Hate speech, or use of disparaging, offensive, threatening language
- Inappropriate or sexual comments on online posts or content

NON-CONSENSUAL USE OF PERSONAL AND INTIMATE CONTENT

Abuse related to the circulation, or threat to circulate through computer means, of intimate, private and/or manipulated images/videos of a woman or girl without her consent.[4]

Images and videos can be

- obtained in a non-consensual manner
- manipulated in a non-consensual manner
- obtained by consensus but shared in a non-consensual way

Blanquerna Universitat Ramon Llull
kaspersky
UNA CASA PER L'UOMO società cooperativa sociale
www.work-with-perpetrators.eu
Regione del Veneto

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

Useful tips to increase digital security

For everyone, every day

Protect your device with a password or PIN: Every device you have, mobile, computer or tablet, should be protected with a password or PIN that only you know.

When choosing a password or PIN, **don't use easily guessed words or codes**, such as birthdays, pet names, or other things you like. Don't use the same password or PIN on every device.

Don't share passwords for your devices and your accounts and profiles with other people, including your (former) partner or children.

Do not save passwords on your computer or mobile phone, or on notebooks, planners or sheets of paper in your home or office. You can securely save passwords in dedicated apps or devices, which are called “password managers”.

Disable the geolocation of your phone or tablet when you don't need it.

Before turning off a device shared with others, **log out and sign out** of sites and accounts, and use incognito mode while using it.

Control your social media privacy settings by choosing the highest level of privacy.

Be careful what you post online, especially if it's content that can reveal your whereabouts or other information or images that could be exploited to damage you or your reputation.

In general, **do not publicly share personal information online** (name, address, date of birth, social security number, telephone number, credit card number, etc.).

When you suspect or are certain that someone is cyberstalking you

Use a secure device, to which your partner does not have access. It could be a new device, a public one, that of a trusted person, or an old phone without internet. The secure device should be used for all communication with the anti-violence center, with the police, with the lawyer, with the doctor, with the bank, etc.

Turn on a new phone number or use a secure number (such as a friend or neighbor's) to communicate with the police, the anti-violence center, and your lawyer. Share this number only with trusted people.

Create a new email account to manage communications. This account will also be used to create other accounts (for the bank, health services, insurance, etc.) and when another email address is needed to verify your identity. If possible, don't use your first name/last name for email, but choose another name (e.g. something@email.com instead of NameSurname@email.com).

Create a new Google or iCloud account for your secure device. It is important to remember that Google or iCloud account stores information about you and your life, such as photos, emails, contacts, files, etc. When you create your new account, follow the rules above to have strong passwords.

Turn off smart devices in your home like Google nest or Alexa, which could be used to listen to conversations remotely.

Use your browser's incognito mode when browsing the internet, so there are no traces of the websites you visit.

Blanquerna Universitat Ramon Llull · kaspersky · Una Casa per l'Uomo · Regione del Veneto

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

ATTENTION!

- If you find that you have a spy app installed on your device DO NOT remove it.
- If you receive threatening or abusive messages, DO NOT delete them.
- And in general, if you find yourself a victim of abuse DO NOT try to solve it yourself!

In addition to eliminating or confusing evidence and material for any present or future legal action on your behalf, this could put you in danger: knowing that you have been discovered, the abuser of the abuse could worsen his behavior.

Instead, protect yourself as follows:

Contact the **cybercrime unit of the Police**, you can also do it anonymously and without the obligation to file a complaint.

Contact an **anti-violence center** to be supported and informed about the different possibilities you have to escape violence and protect yourself.

And remember, seek help using **secure devices**!

Would you like to know more?
Click here to find materials, videos, news and in-depth contacts.

www.work-with-perpetrators.eu/destalk

Riferimenti

1 European Institute for Gender Equality. (2017, June 19) Cyber violence is a growing threat, especially for women and girls. https://eige.europa.eu/news/cyber-violence-growing-threat-especially-women-and-girls

2 CoE GREVIO (2021) General Recommendation No.1 on the digital dimension of violence against women https://www.coe.int/en/web/istanbul-convention/-/grevio-publishes-its-general-recommendation-no-1

3 EIGE (2022) Cyber Violence against Women and Girls Key Terms and Concepts https://eige.europa.eu/sites/default/files/cyber_violence_against_women_and_girls_key_terms_and_concepts.pdf

4 EIGE (2022)

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