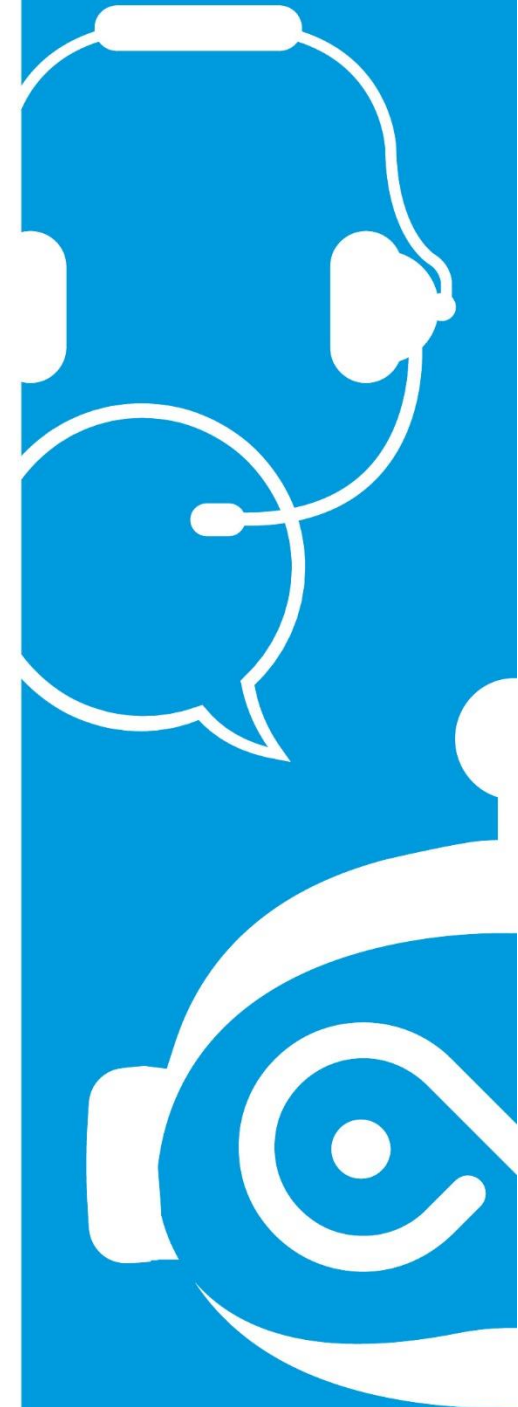




## CYBERBULLYING: DOXXING

### What is it?

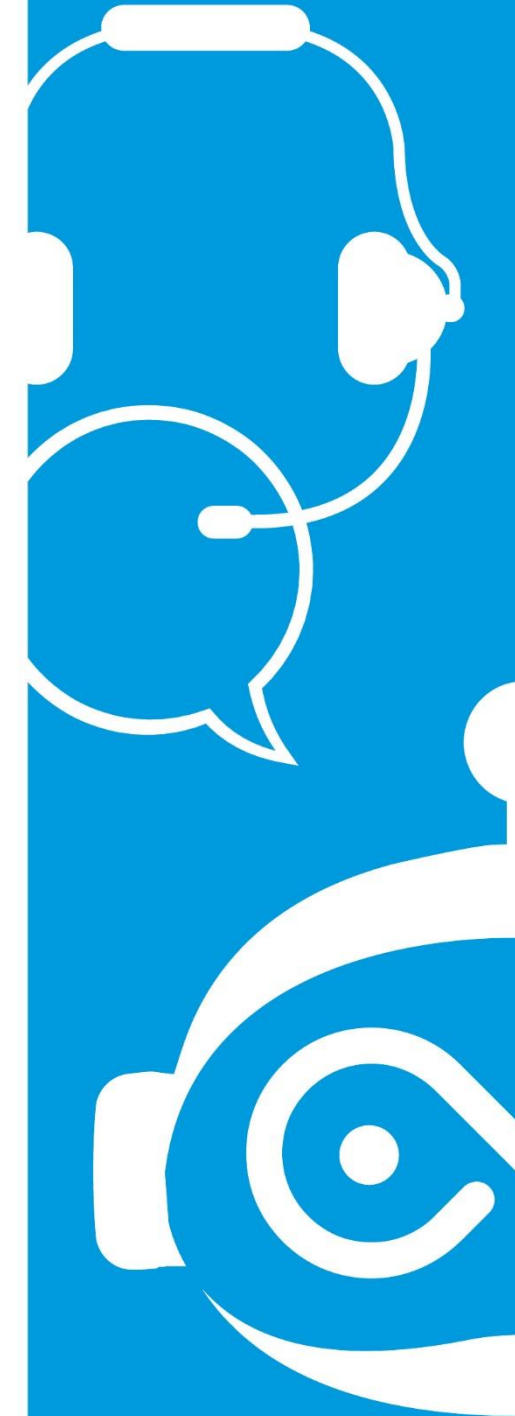
Doxxing is a **digital phenomenon** denoting the act of revealing another user's personally identifiable information online, such as their real name, address, place of work, telephone number, financial or other personal information. This information is then transmitted and spread to the online sphere without the victim's permission. As such, doxxing has been recognised as a form of cyberbullying.



### How can it impact the sexual and reproductive health of youth?

Doxxing can be part of a campaign of harassment against a user with the aim of divulging information of a personal and sexual nature in order to humiliate them. In today's era of social networking, this disclosure is used as a way to undermine the integrity of the individual and negatively impact their mental/emotional health and their livelihood. When it comes to the field of sexual and reproductive health, this can take on many forms.

One of the ways in which this type of doxxing manifests is through the disclosure of private photos without consent or sexual blackmail – threatening to publish such revealing content unless the user complies with certain conditions. Another way in which doxxing can impact SRH is through the practice of 'outing' –the act of disclosing a lesbian, gay, bisexual, or transgender person's sexual orientation or gender identity without that person's consent.



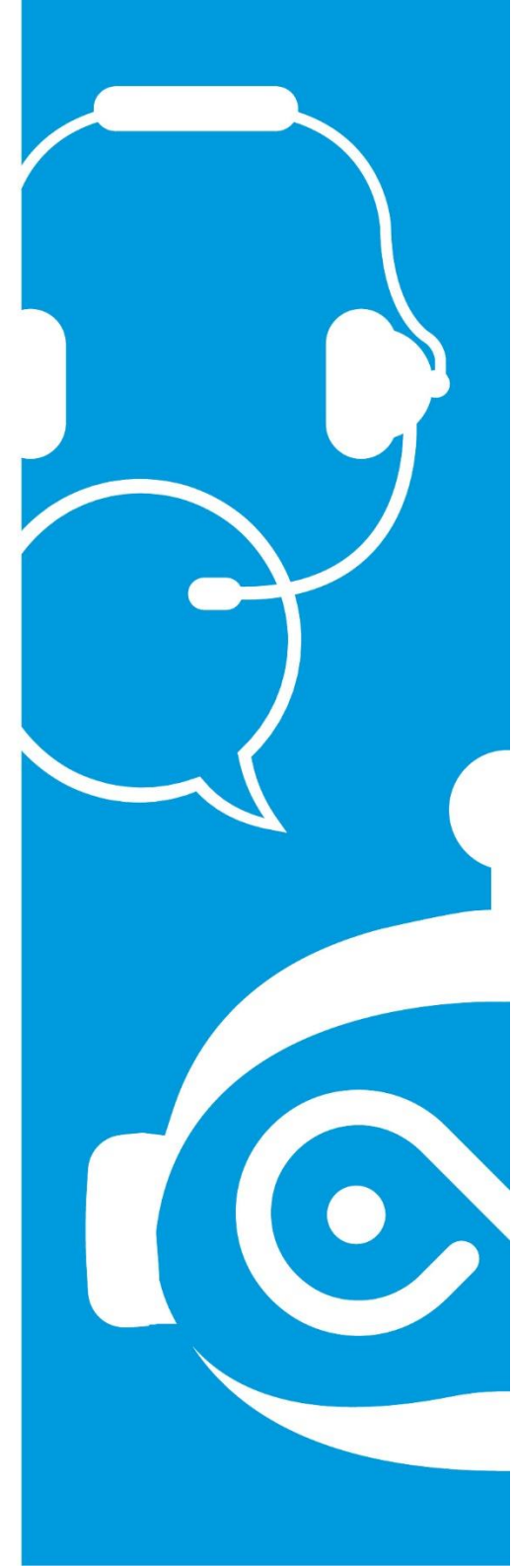
### What are some ways in which youth can be supported?

- Educate youth on the necessity of hiding personal information online and to never share sensitive data if they are not sure about the integrity or trustworthiness of the individual(s) receiving that information. This also means to refrain from posting photos with identifiable markings, from which perpetrators can ascertain personal information such as the school they go/went to, the area in which they live, etc.
- To prevent hacking attempts from those looking to acquire sensitive information, instruct young people to always use strong passwords and never the same ones for different accounts. Having a Google account today allows users to save all of their passwords without needing to remember them.
- Because some apps use location services, young people should always keep these services turned off in their device's settings to prevent a perpetrator from tracking their location.
- Advise youth to only accept follower/friend requests from people they know and to filter their friends/followers more frequently to remove people they don't know or trust to avoid providing unneeded insight to others about their lives.

### Related digital phenomena/tools:

See sheets:

- Gender-based violence: Intimate image abuse
- Privacy: Online anonymity
- Cyberbullying: Cyber stalking



### Further reading:

- Bernard, Colette. "What Is Doxxing and How Can You Keep Your Child Safe?" *Internet Matters* (blog), October 6, 2022. <https://www.internetmatters.org/hub/news-blogs/what-is-doxxing-and-how-can-you-keep-your-child-safe/>.
- Kaspersky. "Le doxing : définition et explication," 2020. <https://www.kaspersky.fr/resource-center/definitions/what-is-doxing>.
- "Online Harmful Sexual Behaviours in Children and Young People under 18 – Position Statement," 2020. <https://www.esafety.gov.au/industry/tech-trends-and-challenges/harmful-sexual-behaviours-under-18>.

