

Introduction

Cyberbullying is when a person uses the internet to harass, intimidate, or threaten someone. Common examples include receiving hurtful or threatening messages, having harmful rumours or gossip spread online, or having private information shared publicly.

Cyberstalking is the use of the internet or digital devices to repeatedly and persistently target, monitor, or harass an individual. Examples can include ongoing unwanted contact across multiple platforms, misuse of GPS or location services to track someone, and in more serious cases, the compromise of accounts or devices to monitor activity.

As both involve harassment in online environments, it is common for elements of cyberbullying and cyberstalking to occur at the same time.

What to look out for

In many situations, it is clear when someone is targeting you with abusive or threatening behaviour online. However, some forms of cyberstalking or online harassment may be less obvious, particularly when they do not involve direct communication. Looking out for both behavioural and technical warning signs can help you identify when something is not right.

Some signs to look out for include:

- ☐ Repeated or persistent messages, comments, or contact from the same person or account.
- ☐ Receiving abusive, threatening, or unwanted messages.
- ☐ Personal information, images, or content being shared online without your consent.
- ☐ Unusual or escalating attempts to contact you across multiple platforms.
- ☐ Changes in behaviour from someone you know that may suggest they are being targeted or coerced online.
- ☐ Alerts or evidence of logins from unfamiliar devices or locations.
- ☐ New or unfamiliar applications appearing on your device.

Sharing & Disclaimer

IDCARE is a not-for-profit and registered Australian charity.

© Copyright Identity Care Australia & New Zealand Ltd. While every effort has been made to ensure the accuracy of the information in this document, IDCARE disclaims any liability to any person with respect to any actions performed or not performed as a result of the contents of this document.

Protecting yourself

What can I do to stay safe online?

- ☐ Report abusive content and block accounts engaging in harassment.
- ☐ Keep records of abusive messages, posts, or interactions in case you need to report them.
- ☐ Review your privacy settings on social media and restrict who can contact you or view your content.
- ☐ Limit the amount of personal information you share online, particularly about your location, routines or relationships.
- ☐ Be cautious when accepting friend requests or messages from unknown accounts.
- ☐ Disable or restrict location sharing features on apps and devices where not required.
- ☐ Speak with trusted family, friends, or support services if you feel unsafe or targeted online.
- ☐ If you have children, talk openly about online behaviour, risks, and how to seek help if they feel uncomfortable or threatened.

How can I make sure my devices and accounts are secure?

In extreme cases, cyberstalking or harassment may involve someone with direct access to your devices or accounts. Taking steps to secure your accounts and devices can help limit access.

- ☐ Secure your accounts with strong, unique passwords and enable multi-factor authentication where available.
- ☐ Lock your devices when not in use.
- ☐ Avoid accessing personal accounts on shared or public devices. If you need to, do not save login details and sign out after each session.
- ☐ If you suspect your device has been compromised, check for unfamiliar applications or settings and run reputable anti-virus or anti-malware software.
- ☐ If you are concerned that your home network may be accessed by others, change your Wi-Fi password and ensure that passwords on network devices (such as modems, routers, and security cameras) are not set to their default values.

Sharing & Disclaimer

IDCARE is a not-for-profit and registered Australian charity.

© Copyright Identity Care Australia & New Zealand Ltd. While every effort has been made to ensure the accuracy of the information in this document,

IDCARE disclaims any liability to any person with respect to any actions performed or not performed as a result of the contents of this document.

Responding – What do I do now?

- ☐ If you or someone you know is in immediate danger, contact emergency services (000 in Australia or 111 in New Zealand).
- ☐ Limit further contact by blocking accounts engaging in harassment.
- ☐ Keep records of abusive activity, including screenshots, messages, and usernames, in case you need to report the behaviour.
- ☐ Report the behaviour directly to the relevant platform so that it can be investigated.
- ☐ Report serious or ongoing harassment to appropriate authorities, such as the [eSafety Commissioner](#) (Australia) or [NetSafe](#) (New Zealand).
- ☐ Seek support and advice from someone you trust, or access counselling services if you are feeling distressed. In Australia, you can contact [KidsHelpLine](#), [BeyondBlue](#), and [LifeLine](#). In New Zealand, you can contact [Lifeline](#), [Youthline](#), and [0800 WHATSUP](#).
- ☐ If you have concerns that your image is being exploited, download IDCARE's [Image Exploitation Fact Sheet](#) for the latest prevention and response advice.

For additional support or information, contact IDCARE:

Submit [Get Help Form](#) | 1800 595 160 (Aus) | 0800 121 068 (NZ)

Sharing & Disclaimer

IDCARE is a not-for-profit and registered Australian charity.

© Copyright Identity Care Australia & New Zealand Ltd. While every effort has been made to ensure the accuracy of the information in this document, IDCARE disclaims any liability to any person with respect to any actions performed or not performed as a result of the contents of this document.