

Introduction

Image exploitation is the use of an individual's image without their knowledge or consent in a way that causes harm. This includes intimate or private images shared with consent but later used beyond that consent, images captured without the individual's knowledge or consent, and images that have been digitally altered or generated using artificial intelligence.

Image exploitation can sometimes be associated with sextortion scams, where threats are made to share the image(s) unless money is paid. In these situations, it is recommended that you cease contact with the blackmailer and block them on all platforms. Do not make any payments. If payment has already been made, it is advised that you do not send any more money.

Prevention Checklist

How can I reduce the risk of image exploitation?

- ☐ Do not store sensitive images on open or low security devices or software. Make sure that the device or images are protected with strong passwords so that only you can access the files.
- ☐ Familiarise yourself with the privacy and security settings on your device and any applications, software or online platforms you are using. Set these to the highest levels of privacy.
- ☐ Be vigilant about who you provide access to your device(s), particularly if they are the same ones you use to store or share sensitive images.
- ☐ When sharing sensitive images, be certain that the individual is trusted.
- ☐ Be future minded - consider whether an image you share could be exploited at some time in the future.

How can I determine if my images are being exploited?

The process of detecting if an image has been exploited can at times be quite difficult. Reverse Images search programs (e.g. tineye.com) can be used to search the web for duplications of an image if you are concerned about exploitation.

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.

Response Checklist

If you or someone you know is experiencing image exploitation, the following checklist can help you to respond.

- ☐ **Report:** Make a request to the platform where the image is displayed to remove content which has been posted online without consent.
- ☐ **Store evidence:** Preserve any information which is related to your content being posted online.
- ☐ **Remove:** The [eSafety Commissioner](#) in Australia has a range of powers to help with the removal of intimate images or videos. In New Zealand, [Netsafe](#) can assist with the process of having the images removed.
- ☐ **Legal action:** It may be possible to take legal action against those who publish intimate images without consent. Report to police and the [eSafety Commissioner \(Australia\)](#) or [Netsafe \(New Zealand\)](#). If the images are of a child and you are concerned that they are in immediate danger, call 000 in Australia or 111 in New Zealand. You can also report online child sexual exploitation through the [Australian Centre to Counter Child Exploitation \(ACCCE\)](#) or report online child exploitation to NZ Police by calling 105 (non-emergency number). You can also report child sexual abuse material to the DIA (<https://www.dia.govt.nz/Digital-Safety-Report-Online-Child-Exploitation-material>). Both the Police and DIA investigate reports of online child exploitation.

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.