

# Image Exploitation

## Image exploitation

Image exploitation is when an individual's image is used without their knowledge or consent to exploit the individual or other entity. Images that can be exploited are diverse and cover instances where leverage can be gained by a perpetrator, including intimate photos, private emails and text messages, and credential information. Images may also be fraudulently used on fake credentials and web sites that sell products.

The impact of image exploitation on a person can be very significant and can be influenced by their willingness to communicate and confide in others, their sense of helplessness, the perceived impacts to them and others, and the seriousness others take in assisting with their response.

### Detecting Image Exploitation





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. Other instances of image exploitation can be more direct, particularly if a perpetrator engages direct with an individual with a view to leveraging their situation for some form of ransom or other benefit.

### Something to be mindful of:

Online data storage services are targeted by criminals and compromises are a common occurrence. Eg. Dropbox experienced a breach in 2016 resulting in thousands of user's accounts and photographs made public to hackers.






## Preventing Image Exploitation

Here's a number of practical measures to consider in reducing the risk of image exploitation:

-  When sharing sensitive images, be certain that the individual or site you are sharing them with/on is one that you trust and is verified.
-  When engaging with online services (e.g. Facebook) minimise the type of sensitive materials you share – assume scammers will be watching.
-  Do not store sensitive images on open/low security devices or software – IDCARE recommends keeping all sensitive information on an external hard drive that is not connected to the internet when not in use.
-  Be future minded – ask whether an image could be exploited at some future point.

# Image Exploitation

## Responding to Image Exploitation

-  **Report:** Companies (e.g. Facebook) will may remove content which has been posted online for you if you request it.
-  **Store Evidence:** Preserve any information which is related to your content being posted online.
-  **Remove:** There are services available which serve to remove online content from the internet for a fee (e.g. dcma.com).
-  **Legal Action:** It may be possible to take legal action against those who publish an individual's intimate photographs without consent. Report to police and if you suspect this involves an exploitation of a child's image contact the eSafety Commissioner (esafety.gov.au).
-  **Seek Help:** Seek counselling/support by [calling IDCARE](#).



## Social Media Security

IDCARE have a number of Social Media Security Fact Sheets to help you detect, prevent and respond to problems you may have. Please see the below Fact sheets on;

-  [Facebook Security](#)
-  [Twitter Security](#)
-  [LinkedIn Security](#)
-  [Instagram Security](#)

## Other Fact Sheets

- |   |  |  |
|---|--|--|
|  <a href="#">Credit Reporting Agencies</a>     |  <a href="#">Engaging Organisations</a> |  <a href="#">Devices and Technology</a> |
|  <a href="#">Scam Prevention and Education</a> |  <a href="#">Social Media</a>           |  <a href="#">Your Rights</a>            |

Disclaimer © 2018 Copyright Identity Care Australia & New Zealand Ltd. While every effort has been made to ensure the accuracy of the information in this FACT SHEET, IDCARE disclaims any liability to any person in respect to any actions performed or not performed as a result of the contents of the alert or any accompanying data provided. Note our service is free to the community and our Counsellors will never ask you to provide your personal information and credentials if we make contact with you.

