Online safety 101

Toolkit for Universities

Creating safer online environments

This resource outlines some of the most common online safety issues and provides advice about how to take action.

Online safety

Online safety is just that: staying safe, online.

Unfortunately, we won't all be safe online, all the time. Any one of us might have a negative experience, ranging from relatively low impact issues like mild criticism or feedback, to more damaging experiences such as cyberbullying (up to 18 years old), adult cyber abuse (18 years and older), image-based abuse or being scammed. This is where the eSafety Commissioner (eSafety) can help.

eSafety's role is to help safeguard Australians at risk from online harms and to promote safer, more positive online experiences. This includes providing advice, information and resources on the eSafety website and helping people who report online abuse.

To help you stay safe online, we recommend following your university's complaint and reporting processes for inappropriate behaviour, supplemented by eSafety's range of recommended safety strategies.

What is adult cyber abuse?

Adult cyber abuse is online communication to or about someone which is menacing, harassing or offensive and also intended to cause serious harm to their physical or mental health.

It can take place in online classrooms, chat and messaging services, social media, text messages, emails, message boards and online forums.

Cyberstalking

Cyberstalking is the use of technology to stalk or repeatedly harass a partner, ex-partner or family member. It is often accompanied by offline stalking. Cyberbstalking may include false accusations, abusive comments, attempts to smear your reputation, threats of physical or sexual violence, or repeated unwanted sexual requests. Cyberstalking may also include monitoring, identity theft and the gathering of information that may be used to threaten, embarrass or harass.

Take action

The eSafety website offers information about cyberstalking, how to know if you are being cyberstalked and what to do if you are the target.

Trolling

Trolling is when someone is deliberatively provocative or inflammatory online and waits for people to take the bait. Examples include people making anti-social comments on online posts which satirise others with the aim of causing offence or provoking a reaction, or posting an image or comment with the aim of frustrating/upsetting others.

Fake accounts and impersonation

Online abusers may set up fake social media accounts pretending to be someone they are not in order to bully, harass or otherwise abuse people. They are also used to monitor and scam people into handing over money, gifts or intimate images or videos. Often these scams are run by organised crime syndicates.

Online hate

Online hate includes targeted and persistent behaviour aimed at ridiculing, insulting, damaging or humiliating a person — this might target someone's physical appearance, religion, gender, race, disability, sexual orientation and/or political beliefs.

Take action

You can report online hate, trolling and fake accounts to the social media service or platform that hosts it — visit the eSafety Guide for direct reporting links. eSafety also provides advice around online scams and identity theft and how to protect your personal information.

Doxing and swatting

Doxing occurs when someone's personal details are shared or publicised online. This may result in offensive comments and unwanted calls or visits from strangers.

Swatting occurs when an abuser makes a hoax call to emergency services to get a large number of police or emergency service responders to another person's address. This can be triggered by a false report of a bomb threat, hostage situation or someone at the address experiencing a mental health emergency, such as being suicidal.

Take action

You can report doxing and swatting to police.

Other types of adult cyber abuse:

Adult cyber abuse can also include:

- sending obscene messages repeatedly to a person or their family, friends or work colleagues
- threatening violence or inciting others to do the same — such as threats of death and sexual assault which may lead to physical contact and/or assault
- encouraging someone to self-harm and/or attempt suicide
- posting or sharing other offensive and inappropriate content — this can include posting inflammatory comments.

Image-based abuse

Image-based abuse is when someone shares, or threatens to share, an intimate photo or video online of you without your consent. The images can be real photos or videos, or ones that have been changed or altered, for example, Photoshopped. It is also image-based abuse if someone threatens to share an intimate image of you without your permission.

Image-based abuse is sometimes also called 'revenge porn'. In many cases, image-based abuse is not about 'revenge' or 'porn'. It is actually a betrayal of trust and shows malicious intent to obtain power and control over someone else.

Statistics show that women are twice as likely as men to have their nude/sexual images shared without consent (15% of women versus 7% of men). Also that a high rate of young adults aged 18 to 24 are likely to have experienced image-based abuse (24% of young women and 16% of young men).

Take action

Visit eSafety's website for information and advice about image-based abuse, including how you can take action. You can report image-based abuse to eSafety and request that images are removed.

Sexual extortion

Sexual extortion is a type of image-based abuse. It is a form of blackmail where someone threatens to share intimate images of another person online unless they give in to the demands. These demands are typically for money, additional intimate images or sexual favours. Perpetrators often target people through dating apps, social media, webcams or adult pornography sites. While sextortion can be used by individuals, organised crime is often behind it when the perpetrator demands money. Commonly the perpetrator is not based in Australia.

Take action

Visit eSafety's website for advice on sexual extortion and how you can take action. You can report image-based abuse to eSafety and request that images are removed.

Help for online abuse

For anyone targeted by online abuse there are a number of ways to address the issue.

Firstly, difficult as it might be, try not to respond or retaliate. People who post hurtful comments and messages online often do so just to get a reaction.

While your immediate reaction might be to make the abusive content disappear, it's important to collect evidence that documents what is happening and report the abuse before you block or delete it. eSafety's advice on collecting evidence can help.

eSafety has legal powers to help protect people who live in Australia from the most serious online abuse and harmful content. This includes content posted publicly or communicated through an online or electronic service or platform, including social media, games, chat apps, emails, messages (including SMS), forums and websites.

Make sure to collect evidence such as screenshots, web page addresses (URLs) and account profiles or usernames before reporting the abuse to the online service or platform where it happened. If they do not help, you can report it to eSafety. Image-based abuse should be reported to eSafety immediately. You can also find out more about our reporting schemes.

Then you can use all the tools available to you to block or mute anyone abusing you. If they reappear on a social media service or platform under a different name, block or mute them again.

Learn more

eSafety has a range of supports for anyone experiencing online abuse.

- The eSafety Guide provides comprehensive information on a range of apps, social media and games, with detail about how to protect your information and report inappropriate content.
- eSafety provides advice on how to report adult cyber abuse to social media services.
- eSafety's has tips on how to manage the impacts of adult cyber abuse.
- eSafety's image-based abuse reporting tool provides step-by-step guidance on how to report the sharing or threat of sharing intimate images/videos without your consent.

If you are in danger right now, contact police on TripleZero (000).

For non-emergencies, you can call the Police Assistance Line on 131 444 or contact your local police station.

Updated 07/2023