CYBER SAFETY STUDENT FACTSHEET

swinburne.edu.au/safercommunity

MADE BY THE SAFER COMMUNITY TEAM

CREATING A SAFE AND RESPECTFUL SWINBURNE COMMUNITY.

The online world opens doors to explore a broad range of information, experiences and ideas. It can be a great way to stay in touch and make new connections but there are also risks. One of the risks posed by the online world is cyber abuse.

Cyber abuse involves the use of technology to threaten, intimidate, harass or humiliate someone. Experiencing cyber abuse can have a profound impact on an individual's social, psychological and physical wellbeing as well as their sense of safety.

Staying safe online

As a Swinburne student, you have a responsibility to contribute to a safe and inclusive online environment by ensuring that your interactions with your peers and staff remain respectful. No matter if you're studying on or offline, the **Swinburne Student Charter**, **IT acceptable use guidelines** and **Social Media guidelines** still apply.

You can access the **Netiquette and Promoting a Safer Online Environment resource** and the **eSafety Toolkit** for more details on staying safe and contributing to a positive experience online for everyone.

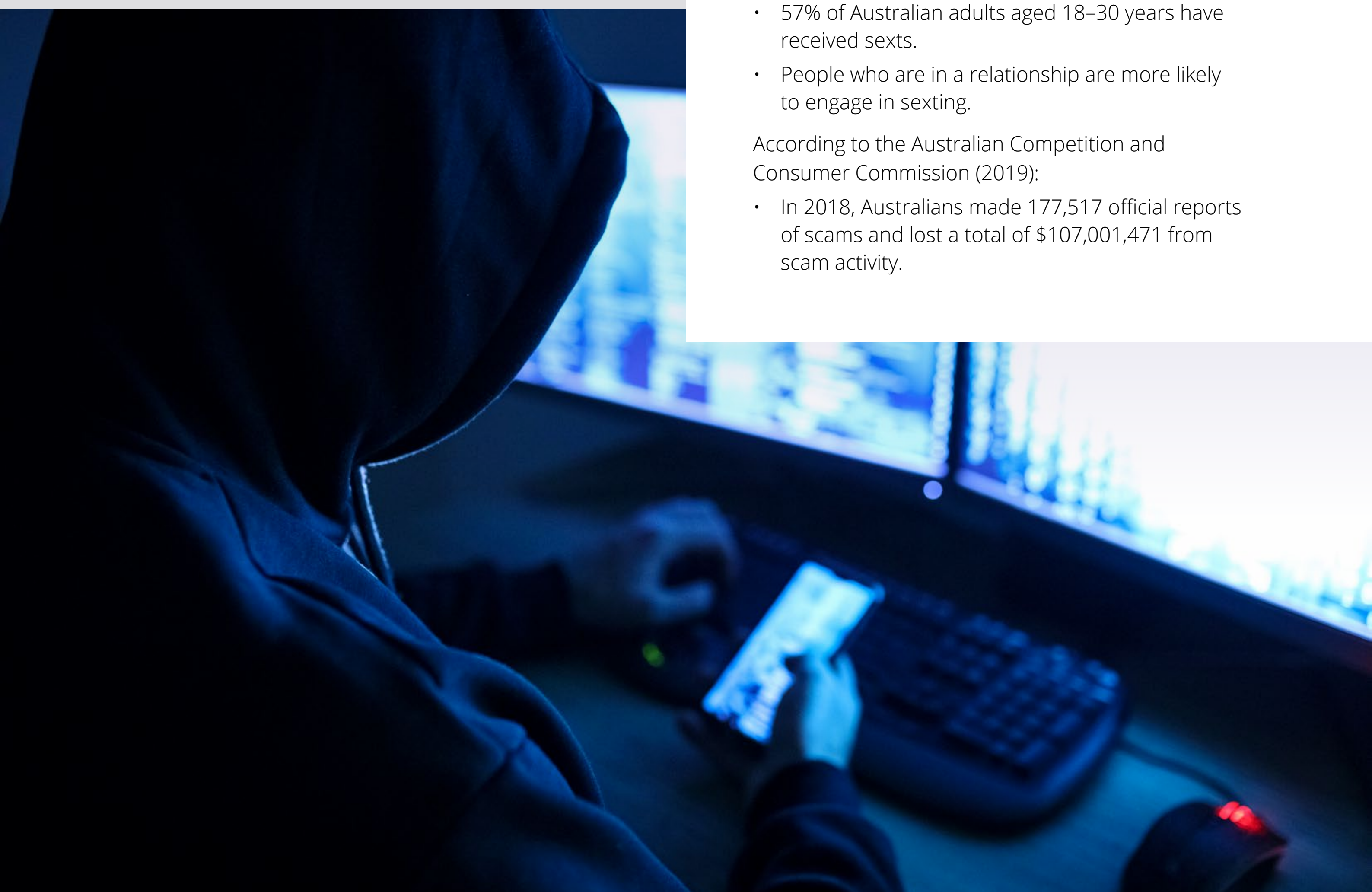
Some statistics (Australia)

According to the Australian Institute of Family Studies (2018):

- 53% of Australian adults aged 18–30 years have sent sexts.
- 57% of Australian adults aged 18–30 years have received sexts.
- People who are in a relationship are more likely to engage in sexting.

According to the Australian Competition and Consumer Commission (2019):

- In 2018, Australians made 177,517 official reports of scams and lost a total of $107,001,471 from scam activity.



CYBER SAFETY

Sexting

Sexting is the sending of provocative or sexual photos, messages or videos. They are generally sent using a mobile phone but can also include posting or sharing online.

Sending intimate photos to someone without their consent can be considered harassment. Sharing intimate photos of someone without their consent or permission is image-based abuse. Possessing intimate images of someone under 18 years old, when you are over 18 years old, can be considered child pornography, even if they were sent and received consensually.

WHAT TO DO ABOUT SEXTING:

- If you regret sending an image of yourself to a friend or partner, ask them to delete it immediately.
- If someone posts a naked photo or video of you online, report it to the **eSafety Commissioner**.
- Report the behaviour to Safer Community who can offer further advice and support.
- Untag yourself in images and/or videos posted online and report them to the social media site.
- Get support from a trusted friend, family member or an expert counselling support service.

Sextortion

Sextortion is a form of blackmail where a perpetrator threatens to reveal intimate images or videos of you online unless you give in to their demands. These demands are typically for money, further intimate images or sexual favours.

Sharing or threatening to share intimate photos or videos of someone without their permission is illegal in Victoria.

WHAT TO DO ABOUT SEXTORTION:

- If you're concerned about your physical safety call emergency services on Triple Zero (000) or contact local police.
- Report sextortion to the **eSafety Commissioner**. They will work with you to get the right outcomes.
- Report the behaviour to Safer Community who can offer further advice and support.
- Don't give the perpetrator any money or additional images. Stop all contact with them.
- Change your passwords for all social media and online accounts, and review your privacy and security settings.
- Get support from a trusted friend, family member or an expert counselling support service.

Cyberbullying

Cyberbullying is bullying via technology, such as – using the internet or a mobile phone to hurt, harass or embarrass someone. It's illegal to bully or harass someone online.

WHAT TO DO ABOUT CYBERBULLYING:

- Send a single message asking the bully to remove the offensive content. Then block them on the social media site.
- Keep any evidence, e.g. screenshots of messages, photos or online conversations.
- Report offensive content on social media to the social media site.
- Ask Safer Community for advice and support.

Scams

Scammers try to steal your money or personal information. Scams are often done by phone, SMS or email. They often look and sound very real.

You may receive an offer that seems too good to refuse or a request to donate to a cause. Or you may receive a friend request from a physically attractive person that you don't know. Scammer activities are sophisticated and designed to make you respond. Don't.

WHAT TO DO ABOUT SCAMS:

- If you suspect something is a scam, you can do an online search of the exact words used to see if it has been identified by others.
- Delete suspicious emails, texts or social media messages.
- Use the 'Report Phishing' function within your Swinburne student email account to report suspicious emails.
- Never send money to someone you don't know or trust.
- If someone offers a prize or gift, do some research online and see if anyone else has flagged it. You can't win a competition you didn't enter.
- Keep your phone's software and computer's anti-virus software up-to-date.
- Keep your passwords secret. Any legitimate communication will never ask for your password.
- If asked for personal information, call them back using numbers sourced from their website or searches not what has been given to you verbally or in an email.
- Think clearly. Scammers can be emotionally manipulative or use a sense of urgency.
- Report scams to SCAMwatch.
- When in doubt, call the IT Service Desk on **(03) 9214 5000** or email **ServiceDesk@swin.edu.au** before you act.

SUPPORT

On Campus support

SAFER COMMUNITY

Safer Community offers advice, support, intervention, and risk management for students who experience or witness inappropriate, concerning or threatening behaviours on or off campus. You can get in touch with the team by email or via the online reporting form:

safercommunity@swin.edu.au

swinburne.edu.au/incident-reporting-form
swinburne.edu.au/safercommunity

SWINBURNE SECURITY

Contact campus security services for emergencies on campus, after hours assistance or for a security escort.

03 9214 3333

CRISIS LINE - OUT OF HOURS

The Swinburne crisis line is available to help 24 hours a day on weekends and public holidays, and outside business hours on weekdays (before 9am and after 5pm).

Call 1300 854 144

Text 0488 884 145

HEALTH AND WELLBEING (COUNSELLING AND PSYCHOLOGICAL SERVICES)

If you are struggling with a personal, emotional or mental health difficulty, whether related to your studies or your life away from university, counselling may help. Register and make an appointment with the counselling services.

03 9214 8483

swinburne.edu.au/counselling

STUDENT SYSTEMS, HARDWARE AND SOFTWARE SUPPORT

Need help with your password, connecting to Wi-Fi or your student email? Need computer or technical assistance and experiencing any cybersecurity issues? Swinburne's friendly and tech-savvy team are here to help you with all your IT needs.

03 9214 5000

swinburne.edu.au/current-students/student-services-support/study-learning-support/student-systems-hardware-software/

Off Campus support

POLICE

National emergency response and reporting.

In emergencies call 000.

police.vic.gov.au

LIFELINE

24/7 phone crisis support and suicide prevention.

13 11 14

lifeline.org.au

EHEADSPACE

A confidential, free and secure space to chat to qualified youth mental health professionals.

eheadspace.org.au

AUSTRALIAN HUMAN RIGHTS COMMISSION

Investigates and resolves complaints of discrimination, harassment and bullying based on a person's sex, disability, race, age and sexuality.

1300 656 419

humanrights.gov.au

ESAFETY COMMISSIONER

Provides advice, strategies and support for cyber abuse, as well as online reporting.

1800 880 176

esafety.gov.au

SCAMWATCH

SCAMwatch is run by the Australian Competition and Consumer Commission (ACCC). Find out more about scams and report scams.

1300 795 995

scamwatch.gov.au

SUT0243_202011
CRICOS 00111D RTO 3059