



Educate
Engage
Inspire



Presented by

**NORTHROP
GRUMMAN**

In partnership with



Module 1

Introduction to online safety

cybertairan.csiro.au



Learning objectives

- Participants will understand the definition and context of cyber bullying.

Dealing with cyber bullying.

Reporting cyber bullying.

- Participants will understand what makes certain types of information private or more sensitive than others.
- Participants will gain an understanding of how to protect themselves online and appropriately use the internet.

Safe browsing.

Social media tips.

Section 1

Cyber bullying

Etiquette

Commonly accepted rules of how to behave online:

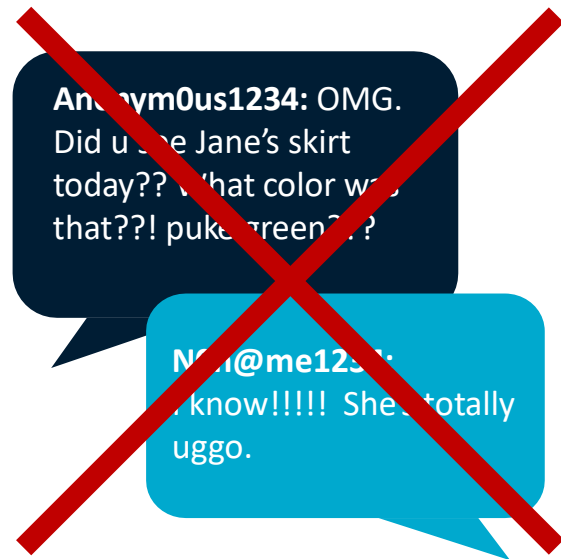
- **Do not** spam forums, chat rooms, or social media sites with useless or repeated information.
- **Do not** pretend to be someone else.
- **Do not** post or distribute illegal material.
- **Do not** use abusive or threatening language.
- **Do not** try to obtain personal info about someone.



~~L3br0nJ@mes: THE CELTICS SUCK! GO MIAMI!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!~~
~~H00psH@N89: Did you guys see the game last night?~~
~~L3br0nJ@mes: THE CELTICS SUCK! GO MIAMI!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!~~
~~B@ll3r4Lyfe: I didn't Miami did alright on D, but they have to work on their 3pt game~~
~~L3br0nJ@mes: THE CELTICS SUCK! GO MIAMI!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!~~
~~L3br0nJ@mes: THE CELTICS SUCK! GO MIAMI!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!~~

Cyber bullying

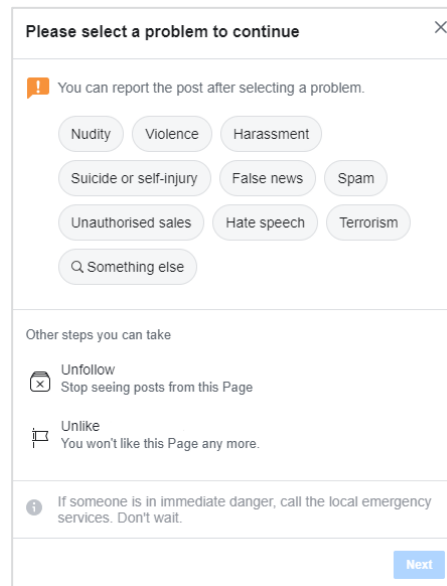
- Bullying refers to any unwanted, aggressive behaviour.
- Cyber bullying refers to any bullying that takes place through use of electronic or digital technology.
- Forms include:
 - Insulting texts or emails.*
 - Rumours sent via email or social networking sites.*
 - Fake profiles.*
 - Embarrassing photos or videos.*
- Why it is harmful:
 - Anonymous.*
 - Can be done 24/7.*



Source: <http://www.stopbullying.gov/cyberbullying/>

Cyber bullying — If it happens to you

- Do not respond to any messages, posts or emails.
- Block offenders.
- Document and report the behaviour so it can be addressed.
- Flag the content so other people aren't hurt by it.
- 1 in 5 Australian young people reported being socially excluded, threatened or abused online.
- 1 in 5 Australian young people (15% of kids, 24% of teens) admitted behaving in a negative way towards a peer online — such as calling them names, deliberately excluding them, or spreading lies or rumours.



The screenshot shows a reporting interface with the title "Please select a problem to continue" and a close button (X). Below the title is an information icon (i) and the text "You can report the post after selecting a problem." There are nine buttons for selecting a problem: "Nudity", "Violence", "Harassment", "Suicide or self-injury", "False news", "Spam", "Unauthorised sales", "Hate speech", and "Terrorism". There is also a search button labeled "Q Something else". Below these buttons is a section titled "Other steps you can take" with two options: "Unfollow" (with a close icon) and "Unlike" (with a flag icon). At the bottom, there is a note with an information icon (i) stating "If someone is in immediate danger, call the local emergency services. Don't wait." and a blue "Next" button.

Source: <http://www.stopbullying.gov/cyberbullying/>

Report cyber bullying

- To schools:

Inform your school of any cyber bullying as you would with other types of bullying.

Provide screenshots or records of bullying.

- To your parents and possibly law enforcement, especially if it involves any of the following:

Threats of violence.

Explicit messages or photos.

Taking a photo or video of someone in a place where he or she would expect privacy.

Stalking and hate crimes.

Source: <http://www.stopbullying.gov/cyberbullying/>

Section 2

Personally identifiable information and online safety

Personally Identifiable Information (PII)

- PII is any information specific to an individual.

- Examples:

Student ID number

Date of birth

Email address

Mailing address

Credit card information



- PII can be used by hackers to steal someone's identity, bank funds, etc.
- Hackers also use PII to impersonate victims in order to gain access to a different persons' or organisations' network.
- This type of information should only be shared with trusted, verified individuals.

Online safety — The basics

- Never share your password.
- Only share PII when *absolutely* necessary.
- Do not download any suspicious or unknown software.
- Always log out when you are done.
- Never post anything you do not want to be public.

You might think you're being safe and limiting your posts to only friends, but anything you post can be easily copied and pasted and sent to someone else.

- If you're unsure about anything you do online, ask your parent or guardian if it is okay.

Risk sites

- Online shopping sites.
- Social media platforms.
- Any other website that requires Personally Identifiable Information (PII).
- These sites are enjoyable and useful. Just make sure you are being extra careful when visiting them.



Safe browsing

- Do not use public Wi-Fi to access risk sites.
- Check the address for spoofs.
- Use a secure website, especially when submitting PII.
- Look for an "s" after "http" in the web address.
- Look for a 'padlock' in the browser address bar.
- Look for a green background or green text.



Browser tools

- Use automatic updates.
- Use and regularly update built-in safety features.

Pop-up blockers

Anti-virus

- Avoid 'save password' or 'remember me' functions.
- Consider using a password manager like LastPass or BitWarden.

Use a STRONG master password (25+ characters)

Use 2-factor authentication



Social media tips

- Be selective.

Only accept or follow friends you know in real life.

- Do not post your location.

- Be careful with apps.

Games and geo-tracking apps may give away your location or other PII.

- Assume everything you post online is permanent.

Employers check social media accounts.

- Don't over-share.

Just because a site asks for information doesn't mean it's required to set up an account.

- Customise and update your security settings.

Default settings are weak.

