



PRESENTATION POINTS

INTRODUCTION

Western Australia Police – 20 Years : Technology Crime Investigation Unit – 2009 to 2014 : Surf Online Safe – 2012 to present.

SOCIAL NETWORKING - RISE IN USE

The number of current users on the Top 10 Apps, by age demographic compared to those of 2014.

Number of people on 1 or more of the Top 10 Social Networking Apps:

42% of children aged 9 to 10 - Compared to 17% in 2014

74% of children aged 11 to 12 - Compared to 27% in 2014

92% of children aged 13 to 17 - Compared to 67% in 2014

88% of Adults aged 18 to 30 – Compared to 78% in 2014

68% of Adults aged 35 to 55 - Compared to 27% in 2014

Discussion Points

- Where most users are falling down is the lack of risk assessment for the use of such networks.
- Many also do not realise the capabilities and “other” aspects of the Apps they are using.

SHIFTING THE CULTURE

We discuss putting rules in place to help build a culture of appropriate use.

1. **Mobile Phone Contract**
2. **Social Media Contract**

Having a contract in place which outlines specific rules and permissions will help continue discussions and offer punishment and reward systems based on how the device is used. Such guidelines are a great way to push the onus of appropriate use to the child.

THE TOP 4 MOST APPS FOR TEENS DISPLAYED AND THE NUMBER OF UNIQUE VISITORS PER DAY IN AUSTRALIA.

Also displayed is the average number of WA students using each App.

1. Facebook

6% of under 18's using. Rarely used by students under the age of 16 years. Low percentage reflected in senior high school students. – Facebook no longer a major factor of concern for WA children.

2. Youtube

24% of students will have their own 'Channel', whereas 90% of students will visit or use Youtube daily or regularly without an account, just on an open visit.

3. Instagram

65% (Primary) to 90% (Secondary) of students are using Instagram.

Discussion Points

- Most students have pushed to Instagram in massive numbers due to the ability to lock down and secure the network more tightly than Facebook allows.
- Less advertising or forced interactivity is a key factor.
- Private Accounts - 92% of Year 5 & 6 students will use private accounts, however by the time they reach Year 11 & 12 this can drop to 68%.

4. TikTok (formerly Musical.ly)

80% of students (Year 5 to Year 10) are using TikTok.

Discussion Points

- Mainly being used by girls to post content, but many boys will use the App to view the girls on it.
- Many predators will trawl the network to interact with young girls. These girls will have non-private accounts because most users hope to become 'TikTok Famous' by gaining massive followers, thus accepting contact from 'randoms'.
- TikTok is the only app which offers a dedicated Parental Control section and option.

5. Snapchat

47% (Primary) to 90% (Secondary) of students are using Snapchat.

Discussion Points

- Over 50% of users are not using or unaware of the 'Ghost Mode' option on Snapchat.
- Users can display their location when posting or using the App on the 'SnapMap' section. As such, if not in private mode, other users can identify the location of another user. Turning off the ability to be seen on the SnapMap is called 'Ghost Mode'.
- SnapChat is the primary app used by teens to send inappropriate images or bullying content..

PRESENTATION POINTS

Social Networking continued

6. Discord

30% (Primary) to 45% (Secondary) of students are using Discord.

Discussion Points

- 90% of users are boys and they are mainly 'Gamers' using the App to interact with their peers whilst they are playing online games.
- Users create their own 'page' and share that link with their peers, inviting them to join the page. They then have a group chat and discuss whatever it is they want.
- Discord is not moderated, as such there is a massive amount of language and content which is inappropriate. This is not a factor though if a user is confined to their own 'page' and does not interact outside of that environment.

7. Whats App

25% (Primary) to 45% (Secondary) of students are using WhatsApp.

Discussion Points

- Mainly being used by 'Gamers' to have live chats with mates while they are playing online games.

8. Omegle

I did not discuss Omegle with the girls in the room as they are quite young. But this site is one which parents need to be aware of. 25% of year 7's are either visiting the Omegle website or are aware of the site - Discussed below.

9. BeReal

12% (Primary) to 40% (Secondary) of students are using Telegram.

- This is very similar to Instagram. You post pics and message peers across the network regarding content. The key difference is when you take a pic on BeReal, both the front and rear camera is activated. This gives the user the chance to share their 'real' environment or experience at that time.
- The app can be set so that Users in a peer group (group chat) have to post a BeReal every day at a time designated by the group. The post window is 2 minutes, so you need to take a pic and post it within that time frame. This can cause issues at school if the BeReal window is set during school hours. It can also cause issues of privacy if people in the pics have not given consent to be in the image.
- If posting to the public open area of BeReal (not peer networks), users location can be displayed in the image. This factor should be deactivated in privacy settings.

10. Reddit

10% (Primary) to 42% (Secondary) of students are using Reddit.

- This has been around for a number of years, but is now also being used by kids to search online content, images and news.
- Many will use as a larger searching option above Google for research content as there are always more results.
- Many male students will use Reddit as a primary source for adult content because it is harder for parents to trace and identify.

Sextortion - Increasing rapidly

I have seen a personal increase of 1100% over the past 6 years for children being sextorted.

Discussion Points

- Boys are usually being approached by randoms in chat environments.
 - Girls are usually approached via social media networks by people they may know indirectly.
1. Online predators – Most offenders are male, but there are many predators using their female partners to entice young males to take their clothes off on the camera.
 2. Scammers – Offenders can be male or female. Many are international and will entice adults and juveniles to engage in a sexual way on cam. They will record the interaction and then threaten to share it publicly unless money is paid or more content is provided.

I provide a detailed online article on sextortion here - <https://www.surfonlinesafe.com.au/sextortion.html>.

Sextortion - Omegle

Omegle is a video chat service which a number of WA kids are using.

I display a screen shot of the site and show a video of how the site works.

With the onset of COVID19, a very large number of students are using the site as a chat option with their mates. However, the site is not what many expect it to be.

Discussion Points

- Omegle is used by a large number of people seeking sexual contact with other cam users.
 - Omegle is one of the most popular sites being used by:
1. Online predators – Most offenders are male, but there are many predators using their female partners to entice young males to take their clothes off on the camera.
 2. Scammers – Offenders can be male or female. Many are international and will entice adults and juveniles to engage in a sexual way on cam. They will record the interaction and then threaten to share it publicly unless money is paid or more content is provided.

PRESENTATION POINTS

Reporting Options

- Esafety Commission website - Civil reporting option and request for removal of content (Bullying and Intimate images).
www.esafety.gov.au
- ACORN website - Police reporting option for any criminal matters : Australian Crime Online Reporting Network
www.acorn.gov.au

TIPS for Parents

We discuss software and hardware based control and monitoring options for families within the home or on childrens mobile devices outside of school.

RESTRICTIONS ON APPLE DEVICES

- Parental Controls and Time Restrictions option on IOS 12/13.
- Family Sharing options can be set up at home.

RESTRICTIONS ON APPLE DEVICES

- Parental Controls and Time Restrictions option on IOS 12/13.
- Family Sharing options can be set up at home.

GET TO KNOW HOW YOU CONNECT TO THE INTERNET

Parental Control options through the home internet connection and Modem.

The vast majority of all modern modems offer parental control options. A user will need to identify the "IP Address" of their modem and enter that into an internet browser address bar. Entering that address into the address bar will open your modem via a simple interface on your computer. The user will then be prompted to enter a username and password in order to access the modem settings. The password and username can be located on the base of the modem, or via the modem manufacturer website.

Once access is made, users can make alteration to control which devices can access the home internet via;

- Access Control
- Web Filtering
- Time Schedules

Further information on how to access your modem can be aquired via your modem manufacturer or supplier (Telco).

OTHER SOFTWARE AND HARDWARE OPTIONS

Parental Control options through the home internet connection and Modem.

- Qustodio
- Our Pact
- The Circle
- The Family Zone
- Family Time

Beacon Cyber Safety App - Free app from the Telethon Kids Institute. A great resource for parents.

All statistics provided have been collected by Paul Litherland

From 2016 to 2019 (inclusive), I have surveyed 7600 students in Western Australia between the ages of 13 to 17 years.

I have recorded extensive notes and gathered statistics during all sessions in regard to specific questions asked of my target audience. Since 2014, over half a million students have seen a Surf Online Safe presentation.

This document and its contents are protected under Australian and International copyright legislation. Reproduction, distribution and display of this document and/or its contents, or part thereof is prohibited without the direct consent of the author - Paul Litherland.