SURF ONLINE SAFE

INTERNET AWARENESS FOR ALL OF US

SURF ONLINE SAFE | W : www.surfonlinesafe.com.au | www.facebook.com/SurfOnlineSafe | E : paul.litherland@surfonlinesafe.com.au

TIKTOK - WHAT PARENTS SHOULD KNOW.

If you have a daughter under 15, chances are she is using TiKTok! Since launching in 2017, Tik Tok has grown massively and was the most downloaded App in 2018, gathering over 194million downloads across the iTunes and Google Play networks. TikTok is an App created in China and designed as an international peer to the massively popular Douyin App, which is based solely in China.

In its first 12 months, TikTok failed to gather much momentum, so the designers purchased rival Chinese App 'Musical.ly' which had already gained massive popularity in the USA, Asia and Europe. In mid 2018 and literally overnight, Musical.ly changed to TikTok and since then it has not missed a beat!

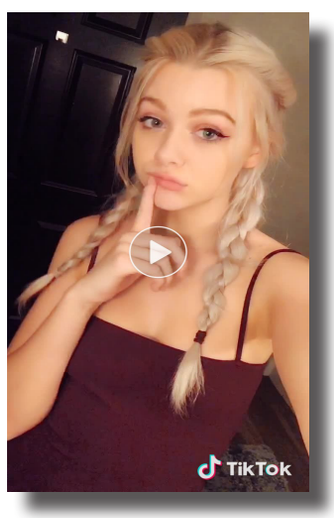
TikTok is a simple App, free to download on IOS and Android. Once you have created an account you can record a video of yourself singing, dancing or lip-syncing to a selection of audio clips. Each video lasts between 3 to 15 seconds and can then be shared across the TikTok network, either privately to your followers or publicly to everyone across the TikTok network.

Users must be over the age of 12 to use TikTok, but a large percentage of the 10 to 12 year olds I speak to, are using it. They should not be, but they are. I do not recommend TikTok to anyone under the age of 13, as it can expose users to bullying and predatory behaviour. In a base sense, TikTok is well designed and if used with an appropriate level of safety and security, it can be a very fun way to interact with your peers.

By default, TikTok accounts are set to public, so when a user adds a video to their account, anyone on TikTok can see it. It is therefore important to change the account settings to 'Private', this way any content posted can only be seen by that users followers. It should be noted that even if a users account is set to private, others can still see their bio, username and account photo, so it is important not to include any identifiable information within those areas. Sadly though, many younger TikTok users will not use private accounts because they want to increase the number of 'likes' on their videos.

When any person posts a video online, other users will judge and criticise that person because of how they look, what they wear or how they are acting. As such, TikTok has one of the highest levels of reported incidents of Cyber Bullying across the USA. People can be very brutal and this is a major reason why younger users should lock down to private accounts.

One of the main concerns for me as a dad and uncle is the predatory aspect of TikTok. Many of our young girls are sharing quite innocent videos of themselves with their friends and followers where they are dancing and having fun, assuming it is similar type users who are looking at them. Sadly (especially if the account is public), this is very often not the case.



A great number of the videos posted by young girls show them wearing bathers or revealing clothing. In a very high percentage of videos, young girls are seen wearing just their pyjamas. Most girls are not posting such videos with any sexual thoughts at all, however there are a massive number of predators on the network who are looking at these young girls and what they are wearing and then trying to make contact with them for interaction of a sexual nature. This is what worries most parents.

It is therefore very important to have conversations with our daughters about how they use TikTok, what they are wearing and especially about how far their videos can go and just who may be looking at them. This will help in reducing risk and raising awareness.

Image - Justine Paradise : 113k Followers

PRESENTATIONS

VISIT WWW.SURFONLINESAFE.COM.AU FOR MORE INFORMATION ON PRESENTATIONS

A Surf Online Safe presentation is not simply about 'Don't do this or don't do that'. It is so much more. Educators and parents regularly offer great feedback on the impact my presentations had on their kids. But what I pride myself on the most is the feedback I get from students themselves. They find my presentation style very relatable and funny, whilst still educational. Students themselves are taking direct action on their online habits as a result of an SOS Presentation and they are discussing it with their peers and parents. For me, this is a great indicator that my message is getting through. This is what I am all about!

Paul Litherland - Owner Surf Online Safe

ONLINE SEXUAL PREDATORS

Choice Target Age Range: 11-14 Years Old

PLENTY OF PLACES TO HIDE

MANY OF OUR KIDS DON'T REALISE HOW EASY IT CAN HAPPEN

Predators are a constant worry for parents. As the online playgrounds of our kids continue to grow, so do the chances of them being approached by online creeps.

Approach can happen anywhere, from social networking to gaming. There are no specific places it happens more than others, but I see it more on social networking (Skype, TikTok and SnapChat) than on Minecraft or Fortnite.

I am not saying it doesn't happen in gaming, but predators find it more difficult to interact in those environments because of the higher risk of being identified and it is harder to hide their behaviour.

Gaming has better moderation than social networking and gamers tend to report or block in much higher numbers. The vast majority of gaming organisations also actively patrol their environments for such activity. Sadly, this is something that rarely happens in so many other web based Apps our kids are using.

Online gamers are at a much higher risk of being groomed by scammers than predators (see Scammers article in this edition).

Predators will hang around places where there is lesser chance of being reported. This is why TikTok and SnapChat are popular with predators. Kids are more open and willing to share and express themselves feely in those Apps. More importantly, they want more likes and followers and this leads to a higher risk of approach.

The most common age of a female target is 10 to 12 and males are from 12 to 14. Girls are targeted in higher numbers than boys at 62% and 36% respectively and over 93% of online predators are male, with 68% aged between 30 & 60 years.

Over the past 10 years I have identified a significant number of online sexual predators target kids who are already vulnerable. They will attempt to share a common interest and this should be something kids and parents must always keep at the front of their mind.

If a young girl is having issues with bullying or isolation, she may post content about it. This is an 'in' for an online predator, as they will make contact specific to that girls concerns in order to build rapport and trust.

Sentences such as "I understand you!", "Forget about the haters, you are beautiful!" or "I get bullied too." are very common introductory approaches from online predators using fake accounts.

Many children mistakenly believe an approach from a predator is quick and their intentions will be clear. So very often this is simply not the case. Many incidents I deal with, the predator can take weeks or months to gain the confidence of a potential victim.

The vast majority of approaches will be for sexual content, such as videos or images. These will be from offenders who are happy to approach kids all over the globe. In the more serious cases, predators will work in the hope of meeting a possible victim for sexual interaction. This will be offenders who live in the same state or city. Though this is rare, it is what parents fear the most.

In a recent Australian survey, 5% of under 18's admitted to visiting with someone they met online. This is a worrying figure, but I believe it is a trend that will continue to rise as online interaction evolves

Most general interactions will last only a few minutes to a few days and offenders will move on quite quickly once they are unsuccessful in getting photo's or vid's.

Others will approach with patience and tact and try to build trust over a period of time. They will often be a higher level offender and will use a number of fake accounts working across many Apps. The longer an online interaction lasts, the higher the risk increases in regard to a possible physical meeting.

This is where we must remain vigilant. Having conversations with our kids is extremely important. Talking to them about minimising their footprint and not accepting contact from randoms is crucial.

Almost 70% of victims have uncontrolled access to the internet on devices in bedrooms. It is amazing how many victims will have conversations with strangers at 1am when parents are fast asleep. I know it is difficult to keep devices out of bedrooms, but there must be rules introduced to minimise this.

Ensuring social networking accounts are set to 'private' is important and not allowing the Apps to share our location is the biggest thing I talk about. Minimising the ability to identify links between your online world and your real world is the key. A predator should not be able to identify where you go to school, where you work or where you live. Many kids share such information quite readily without even knowing it.

Above all, knowing who our kids are chatting with is the most important factor. Regularly talking to them about grooming behaviours must be a priority. Kids who are aware of the possibility of such approaches are more likely to pick up on predators.

If you are concerned your child is being groomed, please contact your local police or visit the Australian Computer & Online Reporting Network at www.acorn.gov.au.

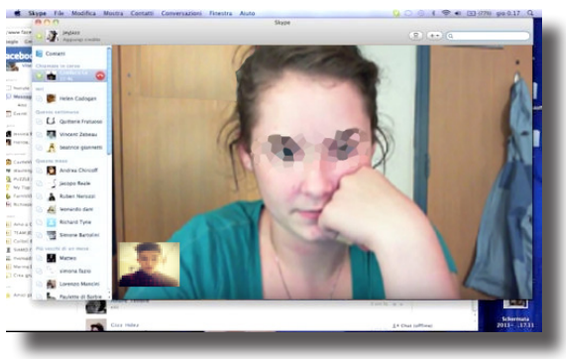
Statistics - Australian Bureau of Statistics

APEX LEGENDS

THIS IS SET TO BE THE NEXT BIG THING - BIGGER THAN FORTNITE!

Fortnite, by Epic Games has been massive for the past 2 years. Any parent of a 10 to 14 year old boy would know all about Fortnite and the huge attraction it created. Well just as Fortnite is starting to drop off and gamers households are getting back to normal, Apex Legends' is on the scene. Run by EA Games, Apex Legends is the latest incursion into the 'Battle Royal' genre. The games are very similar with the main difference being that Fortnite has you fighting on your own, whereas Apex has you fighting in company with 2 of your mates. In its first week of going live (Feb 2019) Apex gathered 25million unique visits and those numbers are rising every day. Keep an eye on my publications for more on this latest gaming trend.

THE NUDES CULTURE



WE NEED TO CONSIDER HOW FAR AN IMAGE CAN GO

The sending and receiving of nudes is a subject I discuss regularly with students, parents and educators. Many online commentators would have us believe our teens are sending nudes all day every day to anyone and everyone, but this is simply not the case.

My research has revealed that 22% of teens from the ages of 13 to 17 will send a nude, this is down from 28% in 2016. These numbers are concerning, but I do not believe they are as high as many would have us believe. A nude is an image or video, where a person is either semi or fully naked. Though girls often share a full body nude, they will rarely show their genitalia. Boys are quite the opposite and will show. In a first exchange, it is rare senders will show their faces, but if sharing continues and the relationship grows, they will take that risk.

Girls are sharing more than boys, with the ratio being 58% and 40% respectively. 39% of girls and 27% of boys will send a nude because they felt pressured to do so. Whereas 42% of girls compared to 71% of boys will send freely without coercion within a relationship. In many cases this does not necessarily mean a sexual relationship, but it is usually between boyfriend and girlfriend.

Teens are expressing themselves in more ways than in the past. Doing it in this form is another method used to interact with someone close to them. Their phone is right there, so getting caught up in a moment is easy. Many girls will send nudes because they feel "confident" or "sexy" from the response given by the person they sent it to. My education to teens, is for them to seriously consider their choices and not to send. But I feel the more important message should be aimed specifically toward where their images may end up if they do send. This is the message I hit extremely hard with all the students I present to.

They may well feel they can trust their partner, and many of them do honestly believe they can. But it is important they understand trust can be broken and as such, control over what has been sent will be lost totally. I emphasise quite clearly that once an image is sent there is no way to truly stop it being shared beyond the person they sent it to. With that in mind, the following statistics are what truly shocks the teens I speak to and more importantly, gets them thinking (girls especially) at how far their images can actually go and who may well be looking at them.

38% of girls compared to just 7% of boys who send a nude, will have it shared by the person they sent it to. Now I am not picking on the boys here, but you can see the massive discrepancy between the sexes in these numbers. Girls will rarely share an image sent to them, but boys will. This is a culture that must change and I am trying my best to do that. So very often I was investigating offences where a girls image was being distributed around her school, often without her knowledge because her boyfriend could not keep it to himself. As a result, many images were ending up on public websites for anyone and everyone to see.

Over the past 6 years, I have spoken to well over 250 thousand teenagers in WA. I am starting to see a marked decrease in the number of nudes being sent because of the messages I give. So it is important to discuss nudes with our teens, especially if they are starting a relationship. These are embarrassing conversations, but they are a must.

Intimate Image Abuse laws were enacted in WA in April of 2019, so it is now against the law to share a nude without the consent of the person depicted. I believe these laws will go a long way in shifting the culture of distribution by teens. A student who may receive a nude will now hopefully consider this legislation and therefore respect the person depicted in the image by not sharing it with their peers. This will be a starting point at least and should get the vast majority of them thinking about consequences.

If you or someone you know has had an intimate image shared without consent please contact your local police or visit the Australian Computer & Online Reporting Network (ACORN) at www.acorn.gov.au. If you identify an intimate image is being displayed publicly online or is being shared through social networking, please visit the eSafety Commission website at www.esafety.gov.au for assistance in the removal of the image.

Statistics - Student survey : Surf Online Safe 2017 to 2018 . 5200 WA students, 13 to 18 years of age.

SCAMMING VICTIMS ARE GETTING YOUNGER!

JUNIOR ONLINE GAMERS ARE NOW ONE OF THE PRIME TARGETS FOR ONLINE SCAMMERS

If you said to me 10 years ago when I first started working at Tech Crime that I would be speaking about young kids getting scammed online, I never would have believed you.

With the huge rise in kids pushing to online gaming environments, they are now being scammed in very large numbers all over the globe and the vast majority of parents are totally unaware it is happening.

If any online game has the option to make purchases through their site, then there is a very high likelihood that scammers will be working through that network to rip off users. It has been happening for years across other online environments, but there has been a massive increase over the past 4 years of kids being scammed through gaming sites.

Close to 27% of children under the age of 16, now have permitted access to a parents credit card for making purchases across the Playstation or X-Box networks. Putting the risk of credit card fraud aside for the moment, pretty much all of the worlds most popular games also have the ability to make purchases within the game itself. This is a trend that has continued to rise over the past 10 years. As a result of this trend, scammers will work across these games themselves with the intention of ripping off users.

Let's use Fortnite as an example, as it is one of the biggest games of 2019 and also had one of the highest rates of reported scams in Australia during 2018. Fortnite is owned by Epic Games USA.

The longer you play Fortnite, the better you get. As you advance through the game, you get better guns, more gaming locations and cooler skins (the clothing you wear). If you do not wish to work through the game to get these things, you can buy them instead. To purchase items within the game, you need to use 'V-Bucks', which is the virtual currency used by Fortnite. A Fortnite player can purchase V-Bucks directly through the Epic Games website or through Microsoft (X-Box) or Playstation. 1000 V-Bucks in Australia will cost you $14.95.

Where most kids are getting scammed is by trying to buy cheap V-Bucks. There are a number of 3rd party websites across the planet which will promote cheap V-Bucks for sale. All of them are dodgy and should be avoided at all costs. Kids will search for these sites themselves or they will see them via advertising on their social networking Apps. As an example, they will offer visitors 2000 V-Bucks for $14.95, instead of the traditional 1000. Kids will then click on purchasing links which will either ask them to enter their Fortnite account details for verification or they will ask the child to submit credit card details for the purchase.

One of 2 things will then happen (or both!) ;

a) The child will lose access to his Fortnite account. The scammer will change the username and password and sell the account to the highest bidder. This is massive across the Fortnite network and can be heart-breaking for many young kids.

b) The credit card will be debited and the child will receive nothing. In most instances it is just the entered amount which is credited, but I have had cases where hundreds or even thousands of dollars have been removed from credit card accounts before parents have had the chance to check.

A great number of the games our kids are playing these days do offer an internal currency or purchasing system. Minecraft has 'Minecraft Coins' and Roblox has 'Robux'. All of these currencies are safe when purchased and used directly through the sites themselves and when abiding by the terms and conditions of the gaming network.

Where most (if not all) victims fall down is when they are making trades or purchases contrary to the advice or T's & C's of the networks. It is very important that credit cards are used with extreme caution across gaming networks. Parents should ensure card details are never saved, even if it is on a secure network such as Playstation. If the card is there kids may be tempted to use it, even if they only think it is a few dollars, this could turn into hundreds.

Sadly most gaming companies and banking organisations will not refund purchases that have been made by children. I have had many situations where kids have used a card without parental consent and the banks have refused a refund because they argue that parent should have secured the card more effectively. One of my cases, a boy of 12 had spent $695 and the bank refused to refund the money.

With over $300million spent on V-Bucks per year across the Fortnite network, this is a massive market for scammers to work in. When a very large percentage of those spenders are kids under the age of 15, it is a goldmine for anyone wanting to make easy money. Parents need to be vigilant and kids need to understand the risks that are out there.