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

INTIMATE IMAGE ABUSE LAWS - FINALLY HERE!

I am very proud to announce that on the 15th of April 2019, Intimate Image Abuse legislation was enacted into WA law. For 5 years I have been a leading advocate for this legislation and I am relieved that it is now finally here. This is a massive step forward in addressing the hundreds of thousands of intimate images being distributed without consent around this country every year. Many of which will end up on public websites for anyone and everyone to view.

The Criminal Law Amendment (Intimate Images) Act 2018, outlines the following:

- An offence for distributing an intimate image of a person without their consent;
- Empower courts to make a 'take down' order in relation to the image; and
- Criminalise the threat to distribute an intimate image.

An 'Intimate Image' is defined as:

- an image of the person naked, partially naked, or in their underwear; and
- an image of a person engaged in a private act, such as a sexual act, using the toilet, showering or bathing.

This legislation pushes the onus back onto those who **receive** an intimate image to make a choice. 'Do I share it?' versus 'Do I keep it private?'

For adults, it gives the option for victims to report such immoral acts to the WA Police and to have charges preferred. In the past, they would have been turned away and simply told it was not against the law. Such a lack of support for victims was totally unacceptable, especially considering how many people are being abused in this way in the online world.

For children from 10 to 17 years of age, this legislation is a great step forward. Not only does it offer a level of support for victims, but (more importantly) it offers a much lesser degree of impact on an 'offender' who may also be under 18. This is the main reason I pushed so hard for these new laws.

Many teenagers in WA who were sharing 'nudes' sent to them by their partners or peers were being charged with Online Child Exploitation offences (child porn) and receiving very harsh and sometimes life changing penalties. Police would therefore rarely charge teens for distributing nudes and as such, many victims (and their parents) would be left without any resolution.

As a result, many high school students in WA were distributing the intimate images of their peers without concern for repercussion. Websites were being created to share them. Victims were being named and shamed and in many cases they were being contacted by predators who had found their images online.

If kids choose to share and the parents of the victim insist Police take action, then at least this legislation offers penalties that are appropriate and will not have a life changing effect on a kid who has made a terrible error of judgement. More importantly, as the legislation is less harsh, police are more likely to take action to get involved, even if it is just to offer a caution or fine. As such, it gives victims a chance to be heard and not to be simply left on their own.

It is my opinion this new law, in conjunction with decent education here in Western Australia, will go a long way in shifting the culture regarding the reckless distribution of intimate images in this state. For more information on this legislation please visit - https://department.justice.wa.gov.au/I/intimate-images-law.aspx.

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

CYBER FLASHING ON THE RISE

A NEW TREND STARTING TO GROW IN WESTERN AUSTRALIA HAS MANY PROFESSIONALS CONCERNED

Over the past 12 months, I have noticed an increase in the incidents of 'Cyber Flashing' in Western Australia. An issue that has been around in the physical world for hundreds of years, has now found its way into the digital world.

Cyber Flashing is when a random person will send an offensive image (usually sexual) to a usually unknown victim, over the Apple AirDrop network. In my experience, the most common places it is occurring is on public transport or within shopping centre food halls.

AirDrop is commonly used to send or receive content across a local environment (work or office) to a number of known recipients. It is a useful tool that has been used effectively for years by iOS users. Not only can you send to other users, but you can also AirDrop to printers and scanners etc. Wherever there is a large group of people, there is the likelihood of a greater number of users having their AirDrop settings set to 'Everyone'. This allows that user to be seen within that local area via a bluetooth or WiFi connection.

A 'flasher' can then scan the area and identify any number of users within a 20 metre range of their device. They can not only assume a potential victim may be close by, but if the victim has used their real name on their device, the flasher can also see who they are.

It is very difficult to trace an AirDrop send, especially if the flasher changes the name of their device immediately after they have sent an image (this is very common). A victim will view the image and see the name of the device that sent it then scan the area themselves to see where that device is, but it is too late as the flasher has already changed their device name.

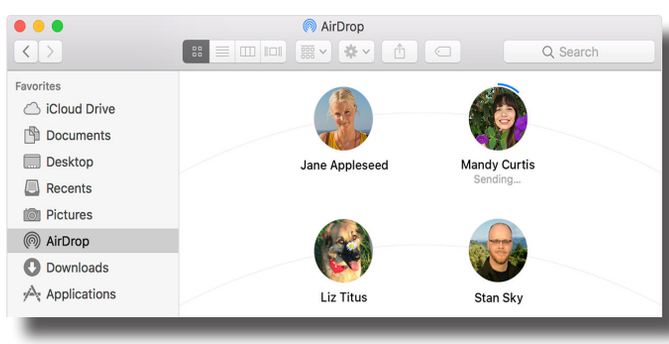
I have also seen occurrences of cyber flashing within some of the schools I present to in Western Australia. Though most schools I have spoken to have not seen evidence of sexual behaviour or content, they have seen this AirDrop method used as another conduit for cyber bullying.

As an example; A group of kids in a class would all be working on their Ipads when a student would send an image or 'Meme' to a bullying victim in the same class or nearby. They would then quickly change their iPad name to avoid detection.

Some schools in WA who are using AirDrop as a teaching aid have implemented a 'No Name Changing' policy in regard to their students IOS devices. If such incidents occur and a student has been seen to change their name, penalties are imposed. This is a great start in minimising this type of behaviour.

AirDrop should be set to 'Contacts Only'. This will stop the ability for a user to be identified and for them to be flashed in this manner.

If you are thinking of giving your child a new iPhone, then sitting down with them and going through the settings on their device in detail will help them understand the risks such environments can impose.



SAFETY TIPS

HOW TO MINIMISE RISK OF EXPOSURE TO NETWORK MARKETING

1. Turn off GPS or Location Services when posting online.
2. Avoid showing links to your location (home, school, work).
3. Become familiar with Trackware & Indexing and how they work (see my other publications).
4. Do not post links or usernames of your other networks.
5. Never use the 'Remember my password' button.
6. Open your FB in one Browser, whilst surfing on another.

LATEST

SOME TOOLS TO HELP YOU STAY SANE

FAMILY ZONE - Some great tools to help keep kids safe. Visit www.familyzone.com for more information. See article in this newsletter re FZ ONE Smartphone.

SNAGIT - A great way to screen capture evidence if your child is being bullied or groomed - https://www.techsmith.com/.

LINKS

SOME USEFUL ONLINE RESOURCES

Cyber Smart - Govt resource website : Visit - www.cybersmart.gov.au

ACORN - The WA Police reporting gateway for online crime : Visit - www.acorn.gov.au.

eSafety Commission - A great site full of usable information and resources : Visit - www.esafety.gov.au

SANITY SAVER AT HOME

GET TO KNOW HOW YOU CONNECT TO THE INTERNET, YOUR ROUTER AND WHAT IT CAN DO

Many parents don't realise methods they can use to help minimise online risk at home. One of the most effective ways of doing this is the use of 'Parental Controls' through your Internet Router. Many modern devices offer such options, using easy to navigate interfaces. You can identify and list each device your child uses and set time schedules for connection to the internet. From 8:30pm to 7:00am each day, you can block everything from the Playstation and Wii, to their Ipad and phone simply by gaining access to the settings in your Router.

You will need to identify if your router does offer such capabilities, if it does not then most leading electronic outlets will have such devices. Once you get an understanding of how changes can be made, you will be surprised at how quickly you will pick up the ability to navigate and make alterations to your home internet connectivity. For a great article and further information on this topic, visit - www.lifewire.com/internet-parental-controls-2487974

LATEST - TELLONYM

HOW CAN THIS STILL BE HAPPENING - NOTE : THIS ARTICLE MAY UPSET SOME READERS.

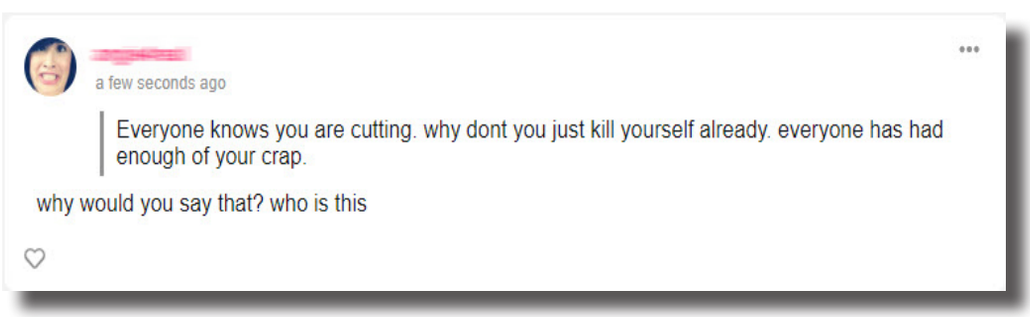
2019, marks the 10th year I have been educating online users on the risks of the online world. Regular visitors to my blogs often hear me say 'enough is enough', 'how can this happen' and 'where is the responsibility of creators'. Hundreds of thousands of Australians have heard my messages and I am regularly inspired by the support I receive here and overseas. But I am getting so frustrated with how often I repeat those statements.

The latest App to show its ugly head in Australia is the German based chat platform Tellonym, which according to one of its co-creators is the 'most honest place on the internet' . A user can create an account with no real joining criteria and simply tick the box that says 'over 17'. You provide an email address (which is not confirmed or authorised) and bingo, you are in! Once your account is created you can send messages or 'Tells' to other users on the network and ask or state anything you want without any moderation or control. What could possibly go wrong?

It is a completely anonymous network and you can say and ask exactly what you want. Tellonym boasts 13 million active users globally and I am seeing it more and more in Australian schools. I am reading the most horrific comments targeting innocent users and it is one of the worst platforms I have seen in some time. Most recently I have read a series of comments targeting a 14 year old girl on the network which would be enough to break the heart of any parent. She had no idea what was being said about her until it was brought to her attention by a peer. She was then exposed to these vile comments and when the perpetrators realised she was on the App, they began to target her directly. As she tried in vain to defend herself, she was subjected to some of the most horrific comments. She was told on numerous accounts she should kill herself, with many users telling her exactly how she should do it.

Tellonym has been designed and launched without any real level of security or safety for users and with absolutely zero moderation. With all we know globally about the effects of cyber bullying on our youth, how can this still be allowed to happen? How can such an App be created and launched with such ease and with little or no safety standards? In the real world you cannot create ANY physical environment without the strictest levels of accountability, safety and responsibility. Yet in the online world, any developer looking for a quick buck can create the most open playground for our kids with zero questions asked. I am trying my best to change this, but I will be honest, it is getting harder and harder to fight this fight.

It is time governments around the world to act on the accountability of such App creators and to start putting truly authentic criteria in place for the creation and policing of such environments and for the true protection of users and non-users. It cannot be left to parents, educators and users to do it themselves.



THE FZONE CYBER SAFE PHONE

THIS IS A MASSIVE STEP FORWARD IN THE CYBER SAFETY WORLD

I have been talking with **Family Zone** for years and this Perth based company are working their butts off. Family Zone has released the worlds first Cyber Safe smartphone and I am excited because myself, parents and kids have been waiting for such a device for years.

The 'FZ ONE' is an Alcatel device (Android OS) available through Family Zone or Woolworths. At $199 it includes 12 months membership to Family Zone. The phone is designed with the FZ software incorporated into the operating system. So you can't use the phone without the safety features as a key component. It offers true 'control' for parents and is a massive step forward in giving the phone's user (your kid), a more realistic feel of freedom and autonomy.

For a number of years now, mobile phone cyber safety has been completely App based. Parents would buy a device for their child and then need to install third party Apps to monitor, moderate and control screen time. Many kids would be able to get around such Apps because parents could never truly control the device. The introduction of the FZ ONE changes the playing field completely, as it provides a foundation of confidence for parents and allows kids to grow with an appropriate culture of use, whilst still being able to enjoy the independence of their own phone.

It is not a brick! It is spot on regarding it's look and design, so kids will be happy to use it. The phone has not been designed by nerds with no understanding of the modern teen, but by parents who are fully aware of the world their kids are in. Not only can you work within the FZ One directly, but you can also view key components of the phone through your own device or computer using the Family Zone App. This is great when you are out and about and the user is at home or at a friends house. 'I am doing my homework Mum!' won't cut it if you can see they have been playing Fortnite and flossing for the past hour!!

Family Zone offer great customer support if you are not technically savvy. So set up is not a worry. I love how the device can offer reports on when, how and where the device is being used. You can also set time schedules for homework and play and set the device to turn off automatically at designated times. It is inspiring that a Western Australian based company has grown to become a global leader with such an initiative and I can't wait to see which other device manufacturers have the courage to get on board and join the fight for true Cyber Safety.

Visit Family Zone - www.familyzone.com/fz-one for more information.

CYBER BULLYING LAWS - IS ANYONE LISTENING?

For almost 6 years, I have been pushing the Western Australian government for the introduction of specific Cyber Bullying legislation. My voice is getting louder and louder, yet those who should be listening are not prepared to hear me. Enough is enough! We need to start considering truly useable options to act on this massive issue in our state.

Over the past 4 years, I have presented to over 70 thousand parents in WA. Each time they are shocked to hear that Cyber Bullying is not legislated in this state. Some of my less knowledgeable opponents will argue there already is legislation available for WA Police to act on Cyber Bullying and as such, there is no need for state laws. This may be correct, but let me explain why that logic is utterly flawed.

The only charge WA Police can use which comes close to Cyber Bullying, is the Federal Offence, 'Use Carriage Service to Harass, Menace and Cause Offence' - Section 474.17 of the Criminal Code Act. Many people argue this piece of legislation is all the police need, but I say it is far more complicated than that.

I worked within the Technology Crime Division of the WA Police for 5 years, working at the coalface of the online world and witnessing first-hand the effects of Cyber Bullying on children. No-one in our office ever charged anyone with 474.17 for one simple reason! I am not going to arrest a 13 year old with a Federal offence! It just doesn't happen. It is way too harsh and carries very strong penalties.

Specific state based Cyber Bullying legislation which is scaled and has more realistic discretionary options for police is urgently required in WA. Laws which can actually be used with ease locally will go a long way in helping the victims of Cyber Bullying, without having a massive impact on offenders. It is not about charging or arresting kids, far from it. If such laws are written correctly and considered appropriately, such action should be the last resort. It is about addressing a specific type of offence which hundreds of thousands of children are the victims of everyday in this country. A cover all, hit and miss Federal charge is not working.

If you or your child is the victim of Cyber Bullying or online harassment, screen capture and document everything! Please do not remain silent. I would encourage you to report the matter to the WA Police by visiting the Australian Computer Online Reporting Network (ACORN) website - www.acorn.gov.au. Please also consider reporting to the Australian eSafety Commission website - www.esafety.gov.au.

We need more voices to push for real change here in WA for effective laws which will help shift the culture of Cyber Bullying in this state.