Keeping kids safe in CYBERSPACE

by Paul Freedman

A CONVERSATION WITH LEE CHISHOLM (NETSAFE)

Space (we've been told) is the final frontier. But a new frontier has opened up in the past decade or two: CYBERSPACE. And, like all frontiers, it's a vast unknown region, filled with challenges, opportunities, threats and dangers.

On the downside, there's the NASTY stuff we keep hearing about: cyber-bullying that targets kids ... scams that fleece innocent adults of their savings ... paedophiles on the lookout for potential victims ... and other traps for the unwary.

On the upside, however, there's the amazing, blow-your-mind, better-than-ever, NICE stuff: the wonderful inter-connectedness that the World Wide Web offers ... the cheap (or free) phonecalls to anywhere in the world ... the online games and movies and music ... and oodles of information on anything-&-everything, all at the click of a button.

What makes cyberspace a bit scary is: it's an ever-changing, still-emerging, rapidly-evolving scene ... and who knows where it's going next? Kids love it, of course, because it's fast, fun, stimulating, exciting. But your average mum and dad can find it hard to keep up.

We recently caught up with Lee Chisholm from *NetSafe*, and asked her what's happening these days online ...

GRAPEVINE: Last time Grapevine featured this subject, *Facebook* hadn't yet shown up, *Twitter* hadn't yet started tweeting, and *YouTube* hadn't yet created the 'YOUniverse'. What difference have these huge global sites made to the Internet and its users?

LEE CHISHOLM: Well, when I started using a computer you'd look up a web page … you'd read it … you'd close it. Then you'd look up another web page … read it … close it.

But then we got something called 'Web 2.0' which was *interactive*. Now, you didn't just look at something and then close it – you looked at it and you *commented*. Or you'd *add* something to it. Or you'd go onto a website and put your *own* information up. You might even start a blog, or a conversation with many people. You might join a group or a forum where you could chat online.

GRAPEVINE: In other words, two-way, rather than just one-way, communication?

LEE: Exactly! When I started at *NetSafe* the young people were on *Bebo* – a site where you could design and decorate your own 'page'. Rather than emailing 10

PHOTOGRAPHER: TAMMY COONEY. MODEL: INDIA-ROSE

IT'S POINTLESS WRITING WITH A BROKEN PENCIL.

friends about what you were doing, you could 'post' your details and photos on your *Bebo* page – so your friends could all look and comment.

Now, of course, 'social media' has become incredibly popular. There's something like 900 million *Facebook* users now. It's vast … universal … which means people who *aren't* on it probably feel like they're missing out.

More and more young people are using *Twitter* – and lots of professionals are there as well, all 'tweeting' their every movement. It's a way of quickly giving your information to a wide audience.

GRAPEVINE: And the difference between a *tweet* and a *blog* is …?

LEE: A *tweet* is only 140 characters … very short and often linked to a blog or to some other site. At *NetSafe*, for instance, we have a *Facebook* page (so people can follow us, see what we're doing). But if we're putting up something interesting on *Facebook*, we'll also *tweet* it, so people following us on *Twitter* can link to our *Facebook* page if they want more detail.

And then there's *YouTube* – a huge reservoir of video-clips. And it's fantastic. You can look up pretty much anything you can imagine. My granddaughter the other day asked me, "What's a dingo?" Instead of trying to explain in words or with still images from an encyclopaedia, I went to *YouTube* – and there was a dingo running across the desert in Australia!

You can look at millions of clips there … post your own videos … even have *your own channel! YouTube* has made people famous – like Justin Bieber, who started off with a little video-clip.

It's the breadth of people who use *YouTube* – the vast range of subjects covered, and the width of audience – that make it so important today.

GRAPEVINE: And what's keeping you busiest at *NetSafe* these days?

LEE: We do a lot of work with educators and schools, especially around cyber-bullying. Scams also keep us busy, with our online reporting button where people report issues to us.

GRAPEVINE: You mean there's a 'button' people can hit when they encounter something worrying?

LEE: Well, not an actual, physical 'big red button' – but there's a website called 'The Orb' (theorb.org.nz) which we run in partnership with other agencies like the Police, the Department of Internal Affairs, the Commerce Commission, the Ministry of Consumer Affairs, the Office of the Privacy Commissioner, the National Cyber Security Centre and NZ Customs. We assess reports that come in, and if applicable we send them on to our partners.

We're also working on a big cyber-security project at the moment.

GRAPEVINE: How best can we protect our computers so, if kids are tempted to look at unsuitable stuff, they'll be blocked?

LEE: Well, the 'clean feed' (which some ISPs, Internet Service Providers, have signed up to in NZ) filters out objectionable material. That's child pornography, in the main, and other undesirable stuff as defined under the censorship rules. But it doesn't filter out porn …

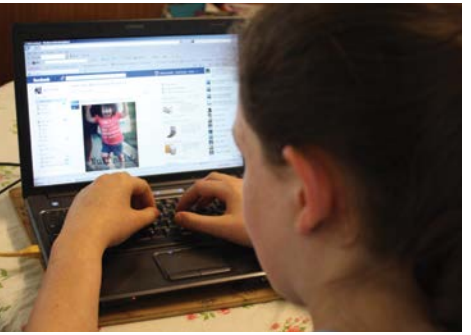
GRAPEVINE: Not porn?

LEE: No. There's nothing *illegal* about pornography if you're over 18. You simply can't stop people from looking at things that are legal. But you *can* put filters on

your family's or your child's computer – and most operating systems now have parental controls to help block pornographic sites, for example.

However, parents need to realise that putting a filter on your computer, no matter how strict it may be, is no guarantee that you'll keep your kids totally safe. Smart phones connect to the Internet – so do *Play Stations, X-Box, iPod Touch* and *Wii* (the gaming system). If your kids want to look at something and they can't get to it on the home computer, they'll go next door or down the road to the Internet café.

GRAPEVINE: Are you saying parents shouldn't even try?



LEE: No, not at all. Just recognise the limitations. When your kids are young, filters work fine. (And some children will never try to get around filters – they'll be quite happy to view only those things their parents approve.) But remember: adolescents are curious, and they're risk-takers. They're busy finding out stuff, exploring who they want to be in the world. And they're experimenting with their autonomy – they'll want to look at forbidden things and push against parental boundaries.

GRAPEVINE: There's a new term now – *'sexting'* – which is kids sending sexually-explicit pictures of themselves to one another via cellphones or computers. Is that common?

LEE: Yes, sending intimate photos to your boyfriend/girlfriend is pretty widespread. And it's not just *young* people. The trouble is, this can easily backfire if that relationship ends. And those intimate photos can easily become common property, popping up suddenly on pornography sites, or sent to employers!

A young person sends an intimate picture to the boyfriend- or girlfriend-of-the-moment and the recipient sends it to "one other person" … he or she sends it to two other people … and before you know it, it's gone *everywhere!* Celebrities have found, to their bitter cost, that a compromising picture can reappear again and again.

GRAPEVINE: So … think long and hard about the worst possible outcomes before you post stuff online?

LEE: Absolutely. And that goes for *any* sort of data – text, not just pictures. You may believe it's only going to your best friend … but you'd better plan for it to go much wider.

GRAPEVINE: How much online scamming goes on in New Zealand?

LEE: It's hard to quantify. There's not a lot of reliable research. But I can tell you there's something like $600 million going out of NZ every year on frauds and scams. (That's an *estimate*, of course – not everyone reports being a victim.)

Dating and romance scams are the most common. Scammers will spend a lot of time – six months even! – talking online to someone they've met in a chatroom or dating site. They'll talk on the

phone, text, build up trust … and the target will think he or she is in love. And then, finally, there'll come some plausible reason why the scammer needs money: for a visa to come here and marry you and live happily-ever-after. ("And I'll bring the jewels I've got with me – I just haven't got any cash!") There are all sorts of inventive stories that people fall for. And it's not just financial loss – there's a painful emotional loss, too.

GRAPEVINE: I heard of an elderly Catholic priest who received an email purporting to come from one of his former parishioners who'd fallen on hard times and "could father please send him some money?"

That sort of thing's happening to lots of people, I presume?

LEE: Oh yes. There are scammers who target Christian or charitable websites, for example. Once they've found someone's email, they can contact them directly and say, "I'm working in Africa for an orphanage and we need money." People's emails and *Facebook* profiles get compromised – and messages are sent out to *everyone* in their contacts list with stories like: "I had to go to London unexpectedly, and I've just been mugged. I've lost all my money. Can you send me x-hundred dollars by Western Union?"

'Western Union', by the way, is *always* a red flag. It's a legitimate money-transfer system, but scammers like it because transactions are completely untraceable. So if you see 'Western Union' in a begging-message, it could well be a scam.

We're seeing a lot more of what's called 'spear phishing' – money-seeking scams targeted very specifically at one person. It's amazing just how much information scammers can find online about people; they'll put a lot of time and energy into this, and their messages can be very plausible and apparently come from someone you know.

GRAPEVINE: What things should alert you to a possible scam?

LEE: No bank or legitimate organisation like *Trade Me* will ever ask you to put your account details, passwords, pin numbers or personal information in an email. *Anything* asking for those is going to be a scam.

"Putting a filter on your computer is no guarantee that you'll keep your kids safe. Smart phones connect to the Internet – so do Play Stations, X-Box, iPod Touch and Wii. And your kids can easily go next door, or down the road to the Internet café."

If your computer isn't secure, you're not safe. So you have to think about anti-virus systems, up-dated operating system, up-dated anti-spyware, strong passwords, etc. We operate a website called *The Net Basics* (netbasics.org.nz) which goes through seven basic things you need.

GRAPEVINE: What are the greatest online dangers for young people?

LEE: They certainly get caught up in online relationships. But most youngsters don't usually have enough money to be profitable targets for scammers. The thing that worries young people most is online harassment and cyber-bullying – being called names, receiving horrible,

OLD IS ALWAYS 15 YEARS OLDER THAN I AM.

nasty texts, having rumours and gossip spread about them.

Someone will make up something, tell others, and before you know it, it's gone everywhere. It's probably *completely untrue,* but that rumour will gather pace as it spreads.

Another thing young people fear is being isolated … being left out of a group. For example, everyone else gets an email or an invitation to a group on *Facebook* or some-such, but the bullied child doesn't. That's a tough one for teenagers in particular, because their social network is really important to them. Being cut adrift from their peers can be very disturbing.

GRAPEVINE: So how do parents help them cope with this stuff?

LEE: Well, it can be a very serious problem. Not all young people find it disturbing. Some just shrug it off, "Oh, they're just idiots – I'm not bothered by this!" But for others it can result in lasting harm, and even contribute to suicide-attempts.

The Law Commission's looking at ways of tightening enforcement – quicker mechanisms to take stuff down off the net – because the longer abusive or bullying messages stay up online, the more damage they do, and the more easily they can be copied and spread.

One of the things we try to do with our online reporting button, *The Orb*, is to get stuff taken off-line very quickly.

GRAPEVINE: Is there much surveillance to detect this stuff? Are there lots of people watching the web – like cops on the beat? Or do you have to wait till someone brings a complaint?

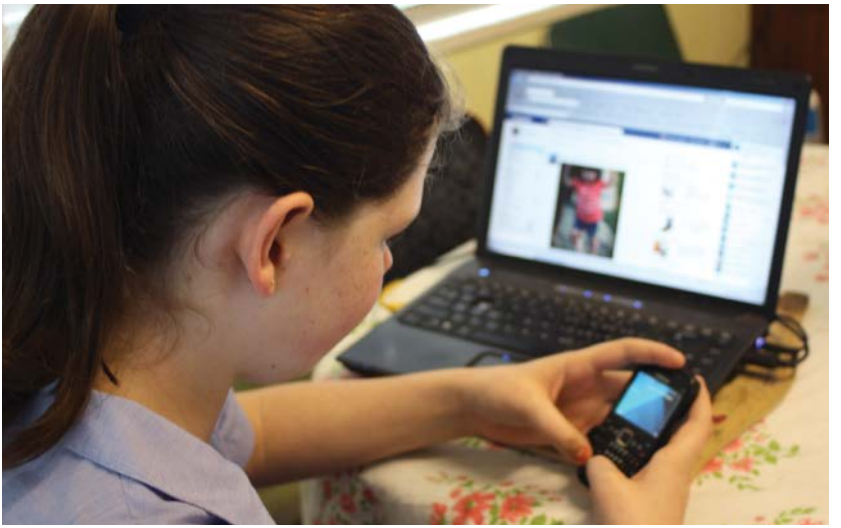
LEE: With nine hundred million people on *Facebook*, no one can possibly check what's happening – it has to be reported. We at *NetSafe* can help with the correct ways to report. The big websites like *Facebook* and *YouTube* are becoming more and more socially responsible – they have to, really. But you have to report the right thing in the right way for it to result in the action you want.

We've a website on cyber-bullying that has a section for parents – cyberbullying.org.nz. You can get to it through the *NetSafe* website, too: www.netsafe.org.nz. There are many other resources out there, all around the world – and there are lots of cyber-safety organisations.

The most important thing parents can do is be *involved* with their young people right from the moment they start using the computer. (In my grandchildren's case, they started at about three or four. And when I got my first smart-phone they figured out how to take photos with it *before I did!)* From the very first time they use this technology, whether they're online yet or not, that's the time to be talking with them about it. And once they start going online, we need to have our rules set out … we need to talk about why this matters, why we don't want them looking at certain types of sites, and so on … we need to make their online activities part of the dinnertime conversation.

Many parents didn't grow up with all this happening, so they're not very comfortable discussing it. But our young people are ALL growing up with technology filling their lives – so it's just vital that parents take an informed interest.

GRAPEVINE: Parents used to be told: "Don't let your child have a computer in their bedroom, and keep the family computer where everyone can see the screen!" But these days lots of families have



"The thing that worries young people most is online harassment and cyber-bullying – being called names, receiving horrible texts, having rumours spread about them. Someone will make up something, tell others, and before you know it, it's gone everywhere."

several PCs, and lots of kids have their own – a laptop or tablet style – as part of their school kit. What's your advice now?

LEE: It's still a good idea, if there *is* a family computer, to have it where adults can drift past every now and then and keep tabs on what the kids are looking at and doing. But today they've got so many other devices and so much ability to connect that you have to TALK to them about it. Just as you'd talk to them about road safety or water safety or the possibility of meeting someone unsavoury on the street, so you have to talk about net-safety.

There's lots of protection in place when kids are very young. But gradually, as the years go by, they need to be able to learn how to protect themselves online.

GRAPEVINE: What do you say to parents who feel they just can't cope with all these new gadgets and sites and 'aps' and so on?

LEE: Well, we see quite a bit of that. We feature websites like 'In My Day' – which is specifically there for parents or adults who feel they simply don't know enough about the technology and what young people are doing. 'In My Day' is in three parts, and consists of little audio cartoon clips that spell out "These are the things young people are doing online … these are some of the challenges they might meet while they're doing it … and here's a bunch of open-ended questions

that might be good to raise with your children."

Some parents have said to us, "We don't even know what to ASK!" Well – this website is there to help them!

GRAPEVINE: Do you get many parents reacting, "It's become such a big, nasty world, and everything's so terribly dangerous, that we're not having ANY of this technology in our home! No TV, no computers, end-of-story!"?

LEE: I sometimes talk to parents who will say, "Oh it's all too awful – we shouldn't have this technological stuff …" But luckily the school will counter, "Well actually they *need* to have it, because we're doing so much of our education online."

It's unrealistic to think that you can keep children isolated. If children are using these devices when they're little, they're much more likely to be talking to their parents – and listening to them. But if they don't get their hands on the devices till they're 14, they're not going to talk to their parents *at all.* They're going to be getting their online contact in secret – and uncensored.

GRAPEVINE: How do you rate the risk of online predators targeting kids?

LEE: Most of the research shows that predators aren't as big a risk as many parents believe. Young people today often say, "Oh, if someone asks us our address, or they ask us to do something sexual online, or they want to send us some sexy pictures or something … we just say no! We just block that person – because why would we?"

So young people on the whole are quite resilient. But not all of them, obviously. There are certainly some vulnerable young people around … and risks exist. But the internet is not crawling with people trying to seduce your children.

I suspect the thing that bothers young people the most is the harassment that happens amongst themselves, and the cyber-bullying they get from their peers.

GRAPEVINE: Are there ways parents can check their children's computers to see what they've been doing? And is that a good idea – or could it cause more harm than good?

LEE: You can certainly install things … not just filters, but monitoring software as well. You can even go to the extent of having real-time monitoring – so you can sit at work (or wherever) and see what your young person is doing online, or even on their smart-phone.

We always advise parents that, "If you want to do this, you should be very open about it." Otherwise, you're spying on your children. And if you see them doing something you don't like, what are you going to do? Say, "Hey, I was spying on you and you've been …!" What does that tell your child? And what does it do for parent/child relations?

Much better to make it transparent. Let your kids know you're doing it.

GRAPEVINE: Are children resistant to this? Do they feel their parents are snooping?

LEE: It depends on their age. The older they get the more they value privacy. By the time you're in your mid-teens you don't want parents, for example, reading your diary. In my day, if I'd had a diary at that age I wouldn't have wanted my parents spying on me or trawling through it. And it's exactly the same thing online.

GRAPEVINE: Well … not quite. A diary isn't a public thing that could attract undesirable contact, is it?

LEE: That's true. But young people will talk about different things in the playground than what they will at home with their parents. And that's normal as they mature.

GRAPEVINE: So parents face quite a challenge, don't they, trying to balance all these factors?

LEE: Yes. And it's very individual to families. Lots of children may have two phones – and parents mightn't even *know* about that second phone. So if there's trouble and they confiscate 'the' phone, they may have no idea the child still has an alternative.

It's probably preferable, right at the beginning, when children are *first* getting access to the technology, for parents to assure them: "Look, there may be things that happen that aren't so good. *Talk* to us about it. *Tell* us! We won't take the technology away from you."

What most often prevents young people being upfront with their parents about online or phone trouble is the fear that they'll lose access. This is their social network … their peer group … their *friends*. If they lose access, then they feel isolated – and that can be just as damaging for them as the things their parents are worried about.

It's far better to say, "Let's work out together what we'll do about a problem, and we won't deny you access." Discuss this before anything happens so they *will* feel that they can come and talk about anything that's concerning them.

GRAPEVINE: To wrap-up, can you leave us with a positive thought about the Internet and Internet-safety?

LEE: The technology's fantastic. It's an amazing tool that can benefit us in many ways. Yes, there are some challenges. And yes, we need, as a community, to be thinking about how we develop good digital citizenship in our children and in ourselves. So as adults we need to model this and be developing those same citizenship attributes in the ways we act *off-line*.

Our young people are growing up *online*, and they'll continue to do so. We need to teach them respect for others … the very same skills that they'll need to get on in the world.

WHAT DO YOU THINK? HAVE YOUR SAY!

GO TO GRAPEVINE'S FACEBOOK PAGE. SHARE YOUR POINT-OF-VIEW AND READ WHAT OTHERS RECKON.

COMMONSENSE ISN'T.