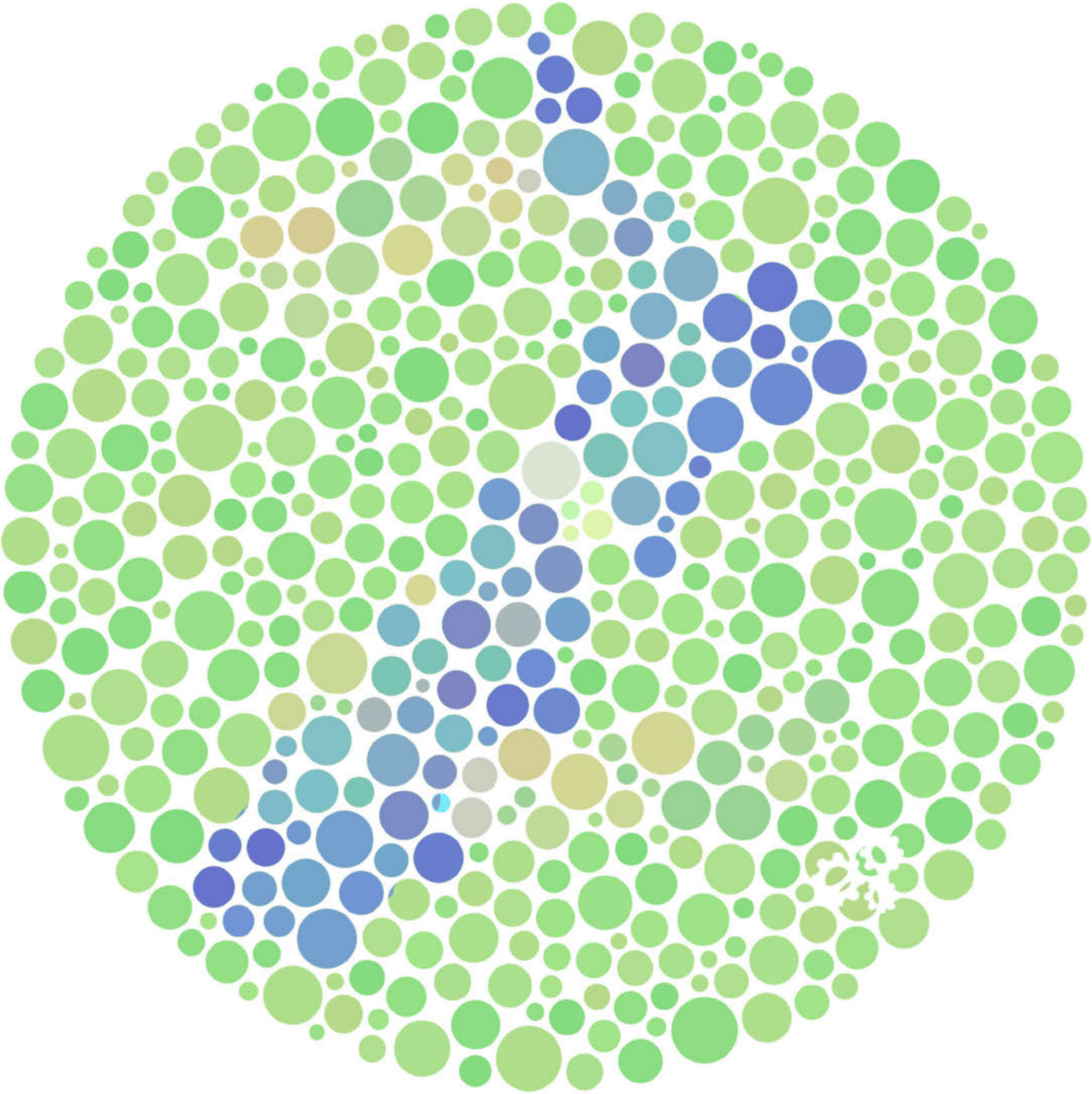
Digital challenge and New Zealanders

A focus on reports made to NetSafe in 2014



A NetSafe Report for Safer Internet Day | 10 February 2015

netsafe

www.netsafe.org.nz

At a Glance

Reports

8121
22 every day

520

520
computer security
incidents
were reported

the average
computer security
incident cost
$10,700

Only
3%
of phishing
reports recorded
resulted in
a financial loss

23%
refered from
NZ Police

30%
came from
Consumer Affairs
Scamwatch

313
reports
of cold-calling
'computer doctors'.
Less than one in ten
resulted in a
loss

1 in 10
reports
involve bullying
or online
harassment

1081
were privacy
related

$8M
in total losses reported

average loss:
$9,300

most significant loss reported was
$1M

the smallest
39 cents

$3.1M
lost to investment scams

20,000
education resources distributed

romance scam victims report loosing
$1.5M

115
training sessions, workshops and conference presentations reaching
4858
individuals

inheritance scams and other advanced fee frauds led to losses of
$1.2m

2400
media articles seen by an audience of over
26M

373,217
visitors to NetSafe's websites

340
schools contacted NetSafe directly for support

Contents

About this report

NetSafe is an independent non-profit organisation that was established in 1998. Its goal is to support the development of a safer and more secure online environment to encourage all New Zealanders to take advantage of digital opportunities.

The opportunities and challenges that New Zealanders experience online have both greatly changed over the last 17 years. In response, NetSafe has adopted a new model for understanding the challenges that people experience when going online called the Digital Challenges Model. This report provides a brief overview of this model and other key ideas related to improving New Zealanders' online experience .

This report also draws from over 8000 requests for help and incident reports that NetSafe received from individuals, businesses and other organisations in 2014. These provide a unique snapshot of the digital challenges that New Zealanders face, and approaches to combat them. It highlights the real-world challenges that all Kiwis can experience online regardless of their age, location or even how 'digitally savvy' they are.

NetSafe believes that this report makes a valuable contribution to the national dialogue already taking place about the digital challenges impacting New Zealand's internet users. This report is written and released with the intention of contributing to the broader development of online safety services in NZ.

Let's create a better internet together

The release of this report coincides with New Zealand's Safer Internet Day 2015. Safer Internet Day is an annual event celebrated worldwide to encourage the safe and positive use of the internet and digital technologies.

A key focus for Safer Internet Day 2015 is to raise awareness about online safety in schools and kura at the beginning of the new school year. Young people are disproportionately affected by online challenges such as aggressive or bullying online communications. However, regardless of their age or background, anyone that goes online can be affected by a range of digital challenges. These include bullying behaviours, viruses and other malware, privacy breaches and scams.

Developing the safe and responsible use of digital technologies is a shared responsibility. It is, and has always been, a multi-stakeholder and multi-sector concern. Safer Internet Day reflects this by bringing together a diverse range of organisations and national programmes to participate in making the internet a safer and better place for New Zealand's families and young people.

The Safer Internet Day initiative serves to highlight the collaboration that occurs all year round between NetSafe and a range of other NZ organisations combating digital challenge.

We encourage others to join NetSafe in creating a better internet.

If you want you to make a contribution to Safer Internet Day in 2016 visit;

http://www.netsafe.org.nz/safer-internet-day/#Section-1

Looking ahead

2015 promises to be a big year for online safety issues in New Zealand. In this report we take a look at some of the key events and issues in the year ahead. The most significant of these is the introduction of the Harmful Digital Communications Act and a revised New Zealand Cyber Security Strategy. The Ministry of Education and NetSafe now host an Online Safety Advisory Group that will attempt to strengthen support of the education sector.

In 2015 New Zealanders will continue to be harmed by the digital challenges that they experience. Much of that harm will be entirely preventable. We must continue to work together to develop a safer and more secure online environment that encourages all New Zealanders to take advantage of the digital opportunities.

Martin Cocker
Executive Director
NetSafe

Rick Shera
Board Chair
NetSafe

10 February 2015

Background | The evolution of online safety

From Cyber safety to Digital Challenge

Increased access to faster more mobile internet connections means that New Zealanders are spending more and more time online. As a result, they are exposed to constantly evolving challenges that include online bullying and harassment, employment and investment scams, cyber attacks and privacy issues.

Cyber safety issues emerged with the rapid penetration of the internet and mobile phones in the late 1990s and early 2000s. The understanding of these issues has evolved since then as developments in digital technology have enabled new, or evolved existing, risks to New Zealanders online. Now cyber safety is thought of as being one of three broad areas of 'Digital Challenge' that also include cybercrime and cybersecurity (the '3Cs').

In the real world these areas of digital challenge overlap. This is simply illustrated in Figure 1.

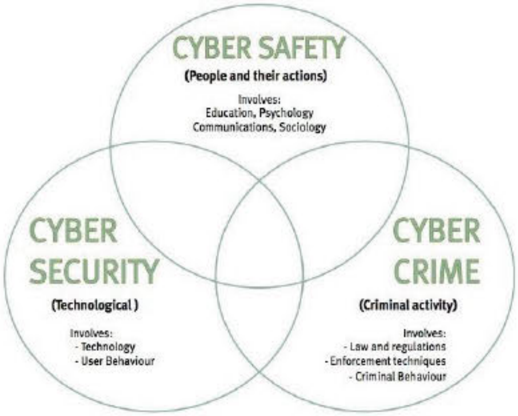


Figure 1. The overlap of digital challenges

Digital Challenge - the '3Cs'

- **Cyber safety:** Involves conduct or behavioural concerns. Examples include cyberbullying, smear campaigns, accessing inappropriate content, being taken in by a scam, creating spoof websites or sexting.
- **Cyber crime:** Involves illegal activity. Examples include, sexual offending, accessing objectionable content or online fraud.
- **Cyber security:** Involves unauthorised access or attacks on a computer system. Examples include hacking into someone's social media service account, launching a Distributed Denial of Service (DDoS) attack or loading malware onto a laptop.

The Digital Challenge Model provides a basis for of understanding the broad range of online safety, security and crime challenges confronting New Zealanders. It also reflects the broad expertise and deep knowledge of the many organisations that work on behalf of New Zealand's internet users; many of which are highlighted in this report as part of NetSafe's partner network.

Increased online opportunity = Increased digital challenge

New Zealanders have almost universal access to the internet and the immense range of benefits that this brings. As a nation of keen internet users, we increasingly expect to be able to connect to the internet no matter where we are or what we are doing. Each day we make use of digital technology to broadcast to our networks, respond to messages, shop or socialise with others. We have come to rely on the versatility of the internet in a very brief period of time.

Going online more often also increases our exposure to digital challenges. All internet users need the knowledge and skills to keep themselves and others safe and secure online. This applies regardless of age, location or occupation and whether going online at home, at work or for play.

The most recently available Statistics NZ data[1] on household internet usage indicated New Zealanders' lack of confidence in internet security is a barrier to them using the internet for social networking and trading goods and services. Perhaps more concerning, is the number of New Zealand households that reported not having an internet connection because of their lack of confidence, knowledge, or skills[2]. More recently, a report from the National Cyber Policy Office indicated that nearly one third of New Zealanders feel that they don't know the steps to take to increase their cyber security[3]. This finding also highlights the large number of people going online regardless of whether they understand the risks.

New Zealand is making great progress towards creating great connectivity and access to motivating and engaging online experiences. However, there is a great deal more work to be done in developing the digital capability of the nation's internet users. For New Zealand to become a truly world-leading 'digital nation' it is not enough to just be connected to the internet. We also need to become a national of skilled 'digital citizens'[4].

[1] Household Use of Information and Communication Technology: 2012. Statistics New Zealand, April 2013

[2] ibid.

[2] ibid.

[3] Research into cyber security behaviours and campaign awareness for 'Connect Smart' 2014. National Cyber Policy

[3] Research into cyber security behaviours and campaign awareness for 'Connect Smart' 2014. National Cyber Policy Office, July 2014

[4] For examples of measures refer to OECD report *Measuring the Digital Economy A New Perspective (December 2014)* and interactive tool at http://www.oecd.org/sti/measuring-the-digital-economy-9789264221796-en.htm

New Zealanders are experiencing Digital Challenge on a daily basis. These range from simple to complex and often span more than one of the 3Cs.

For example, a lack of training or awareness about how to identify and manage a phishing email received at work could result in a unwitting data breach, the payment of company funds to a fraudulent overseas bank account or a malware infection that takes down the entire network.

As digital technology gets more accessible and becomes ever more embedded in our daily lives, it is essential that New Zealanders have the knowledge and skills to tackle the digital challenges.

We all think that we will never be taken in. However, it is increasingly difficult to discern what is real online. So how easy is it to recognise a fly-by-night website selling prom dresses that will never be delivered or understand that a social media message from a close friend suggesting that you 'click here' has been spoofed?

What if a photo shared with a partner is later published online or, if it was intimate, used to blackmail you for more images? Would you know who to contact?

From ‘protecting users from risk’ to ‘enabling Digital Citizens’

In the early days of the internet the response to cyber safety issues was often based upon assumptions instead of research. It was a problem thought of as almost exclusively affecting children. This response was modelled on ‘traditional’ media dangers such as exposure to inappropriate sexual content or ‘stranger danger’. Typically, protections were put in place to restrict access to online content and services. However, as already discussed, rapid changes in digital technology have enabled new, or evolved existing, online challenges. These are primarily related to conduct concerns such as harmful communications, inappropriate ‘digital footprints’ and criminal enterprise. The other important change to note is that these challenges can no longer be thought of as just impacting on young people.

In general, prevention approaches that rely on technical protections, such as content filtering or activity logging, simply do not work. It is essential that internet users also develop the skills and knowledge to keep themselves and others safe online. This includes knowing how and where to seek support when things go wrong. In an increasingly digital world could these competencies now be necessary for a successful life?

These ideas have taken hold in the education sector since NetSafe introduced its definition of a ‘digital citizen’ in 2010. The Digital Citizenship model provides a way of expressing the norms of appropriate and responsible behaviour that a society expects when using digital technology. These ideas do not just apply to schools. They are directly relevant to wider society.

A digital citizen:-

- is a confident and capable user of digital technology
- can identify digital challenges and effectively manage them
- uses digital technologies to participate in economic, educational and cultural activities
- uses critical thinking skills when online
- is literate in the language, symbols, and texts of digital technologies
- uses digital technology to relate to others in positive, meaningful ways
- demonstrates honesty and integrity and ethical behaviour when using digital technology
- respects the concepts of privacy and freedom of speech in a digital world; and
- models the values of digital citizenship

This model simply provides a way of describing the skills, knowledge, values and attitudes that we would want to see in ourselves and others we interact with online. Find out more about the Digital Citizenship model by contacting NetSafe directly at SIDreport@netsafe.org.nz

Education, Response, Advocacy | The evolution of safety services

Online safety organisations set up in the late 1990s and early 2000's were primarily tasked with online safety education. The aim was to make people aware of the 'dangers' so that they could be avoided. It soon became clear that it was not possible to both participate fully online and avoid danger.

Preventative education remains an important component of the response to online safety challenges. However, even when resourced appropriately, an education-based strategy will not be entirely effective. There are some harms that cannot be prevented just by increasing an internet user's skills and knowledge. NetSafe's operational experience shows that problems can result from risk-taking behaviour, an error of judgment or being targeted regardless of the safety and security precautions they have taken.

Increasingly, people experiencing negative incidents sought out agencies that could provide more specific advice and services to assist them. The evolving and increasingly complex nature of many digital challenges meant that traditional support and enforcement services were increasingly unable to provide assistance.

Internationally, online safety agencies providing a particular blend of services were increasingly being sought out because of the deep specialist knowledge that they were developing. This includes an understanding of the digital challenges, how to tackle them and who to work with to achieve this. Essentially, the work of agencies like NetSafe now takes place at the intersection of the '3Cs' to provide services across three broad areas:-

- **Education** - Independent, quality advice and guidance to individuals and public, NGOs and commercial sectors. Support other organisations to develop educational resources, response services and other interventions.
- **Response** - Direct assistance in response to incident reports. Facilitate access to a range of support mechanisms. Work across sectors to strengthen the overall reporting processes available to New Zealanders.
- **Advocacy** - Expert knowledge grounded in both research and real world experience. Advocate on behalf of the community's safety and security needs to see that these are reflected in legislative or government policy changes and provide expert knowledge to policy makers.

In 2015, NetSafe directly supports consumers, families, schools and businesses as they navigate through a range of online 'digital challenges' - financial, technical and emotional. It helps them to reduce their exposure to risk or to minimise harm when things go wrong. NetSafe responds to over 700 requests for support each month received via a range of communication channels. It also provides workshops and expert advice around the country.

The 2014 digital challenges report

About the data in this report

This report is based primarily on data from the queries and reports that NetSafe received from individuals and organisations in 2014. These were either seeking advice on prevention or on how to reduce harm when an incident had already occurred. NetSafe receives reports related to inappropriate online conduct, criminal offending and infringements of civil law.

NetSafe records any financial loss resulting directly from online fraud or other scam reported to it. It should be remembered that the figures provided do not include incidental financial loss incurred during the recovery from a problem. Neither does it reflect other, non-financial, types of harms that people can experience. In particular, the concept of emotional harm is recognised in the Harmful Digital Communications (HDC) Bill 2014 currently before parliament. This type of harm can result from, for example, online harassment of adults or young people.

NetSafe manages reports and queries involving both financial and non-financial harm. For example, in one scam reported to NetSafe a New Zealander handed their life savings over to an overseas criminal. The emotional toll of being 'taken in' was combined with little hope of recovering the money, convicting (or even identifying) the perpetrator. This had an significant impact on the victim and their wider family as they provided support and worked to make up the original loss.

NetSafe estimates that only a small percentage of the incidents experienced online are reported. As such, the data in this report is representative of the experience of many more New Zealanders.

Examples of reports made to NetSafe in 2014 are provided. These should give an insight into the wider, and much more difficult to quantify, impact of non-financial harm that is experienced on a daily basis by those targeted by bullying and online harassment across New Zealand.

For more information on the data and incident information provided in this report please contact NetSafe directly at SIDreport@netsafe.org.nz

Inter-agency referrals

NetSafe works with a range of New Zealand government agencies to manage the reports and queries made by New Zealanders to them each day. This is perhaps best illustrated by NetSafe's work on the Online Reporting Button (ORB) website service[5]. NetSafe launched the ORB in 2010 as an online channel

[5] http://www.theorb.org.nz

for New Zealanders to report cyber incidents. Current ORB partners are the New Zealand Police, Department of Internal Affairs, Privacy Commissioner, Consumer Affairs, Commerce Commission, National Cyber Security Centre, New Zealand Customs Service and Trade Me.

NetSafe ‘triages’ the reports made to the ORB and refers them on to the appropriate agency for action. Since 2012, NetSafe has partnered with the Ministry of Business, Innovation and Employment (MBIE) to deliver the Consumer Affairs Scamwatch service[6]. Scamwatch referred 2425 reports to NetSafe in 2014, or 30% of the total received, via phone, email, social media channels and the ORB.

A further 23% of all reports (1878) were directly referred by the New Zealand Police to our free helpline service or to the ORB system. NetSafe triages these reports and works with specialist police units to escalate priority cases for their investigation. In particular, NetSafe works with the Police National Cyber Crime Centre (NC3), Online Child Exploitation Across New Zealand (OCEANZ) unit and also fraud investigators in the Auckland region.

NetSafe’s partner network

The management of inter-agency referrals highlights the importance of a partnered, cross-sector approach to combating digital challenge. To be effective across the Education, Response and Advocacy workstreams, NetSafe draws on a broad partner network of national and international organisations for assistance.

NetSafe acknowledges the expertise and experience provided by the people at these organisations, and for their work throughout the year combating digital challenge across the ‘3Cs’. A list of partners is provided at the back of this report.

[6] http://www.consumeraffairs.govt.nz/scams

Digital Challenge | The impact on New Zealanders

About the reports and queries NetSafe receives

NetSafe recorded more than 8000 reports and queries in 2014. An average of 22 every day of the year across all types of digital challenge. Of these, NetSafe received over 850 reports involving a direct financial loss. The total reported loss was nearly $8 million.

NetSafe receives many reports about issues that are outside of its remit. It refers these to the correct agency and these are not included in the data. Examples from 2014 include reports on immigration fraud, noisy neighbours, dog nappings, graffiti, overcharging in shops, road rage, burglary, domestic violence and illegal firework sales.

NetSafe categorises the reports and queries it receives against the three types of digital challenge. Other queries related to NetSafe's business such as those from the media, requests for education resources or consultancy services make up nearly 11% of the total.

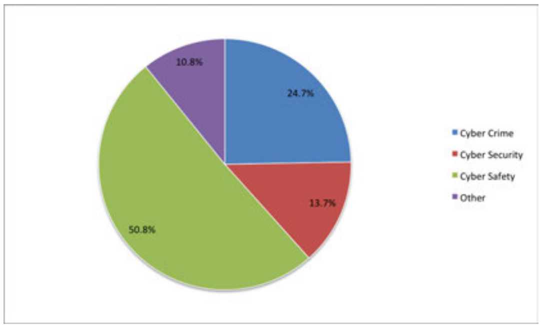


Figure 2 Incident reports categorised by digital challenges classification

As noted above, the boundaries between the three types of digital challenge can be blurred and involve aspects of cyber safety, security and/or criminal activity. NetSafe categorises the reports or queries it receives on a case-by-case basis by assessing the dominant factors involved.

'Cyber safety' constitutes the largest proportion of incidents primarily because this category includes online fraud and scams. This is because successful cyber crime and cyber security incidents often require someone to make a mistake (e.g. click a link or enter credit card details). Therefore when the most significant contributing factor in incident is a user's action, such as in an online scam, it is categorised as 'cyber safety'.

Reports involving emotional harm

It is extremely difficult to measure the impact of many negative online experiences. Whilst up to 20% of secondary school age students report being cyber bullied, and up to 10% of adults report being harassed online, only some of them will suffer serious harm as a result. Examples of this type of incident are provided in this report. In each case NetSafe triaged the report and either referred or managed it to its closure.

Every month NetSafe receives approximately 80 complaints that directly relate to aggressive, threatening, intimidating or bullying online behaviours. Usually people contact NetSafe when they feel a situation has escalated out of their control. Often they have tried other options or have been referred to us from another agency. At this point, regardless of the severity of complaint, they believe that there isn't a solution to their problem. In virtually all cases there are clear indications of emotional stress and, often, distress.

The specific characteristics of these complaints, and the context in which they occur, lend them to a meaningful level of resolution between both parties to a complaint. Existing self-regulatory remedies, such as the uncontested removal of harmful content, can bring some relief to victims when certain conditions must be met.

Agencies like NetSafe can assist to remove the feeling of isolation, and provide a roadmap for the overall response. However, the reality is that currently available options are limited both in scope and effectiveness. The HDC Bill, due to be passed in 2015, has the capability to dramatically change this equation.

Most significant social media service providers already enable users to request the removal of offensive or harmful content. However, the threshold for action varies across providers as does the quality of their support services. For an individual who is targeted by multiple users on multiple platforms, this can be a very difficult and stressful process to navigate.

The Harmful Digital Communications Act will assist by:

- Introducing a standardised process for dealing with offending content,
- Focussing responsibility for resolution on the user that posted offensive content and,
- Appointing an agency ('the Approved Agency') as the official first point of contact.

Aggressive and bullying online behaviours

Over 10% (921) of the reports NetSafe handled in 2014 involved bullying behaviours or online harassment that would qualify for assistance from the Approved Agency under the Act. Current legislation offers some ability to address harm caused to people that, for example, report fake profiles, threats or abuse online.

NetSafe also acts to mitigate the impact of these digital challenges by working with many of the leading international online organisations to remove content where feasible. These existing processes are the basis for the Approved Agency services as defined in the Bill.

Breaches of the Privacy Act

Digital technologies have made it extremely easy to breach individual privacy. With mobile devices and access to the internet nearly ubiquitous, a private moment can be captured and shared publicly in seconds. Unprecedented amounts of data are being captured about individuals, presenting opportunities for the deliberate theft, or accidental release of private information.

Many harmful communications cases have multiple components that each have the potential to infringe the law. The current scope of the Privacy Act and the Privacy Commissioner's Office function means victims often use ‘privacy breach’ as a catchall for a range of issues, because it presents an pathway for action. As a result, a significant portion of the reports to NetSafe included a privacy related issue, and NetSafe has developed a close working relationship with the Office of the Privacy Commissioner.

NetSafe recorded 1081 privacy related reports (13% of all reports) in 2014. Many of these were referred to the Office of the Privacy Commissioner for evaluation in their role as an ORB partner. For example, NetSafe received multiple complaints of identity theft related to the Profile Engine website resulting in a published decision from the Privacy Commissioner and further guidance for complainants being issued[7].

[7] Profile Engine deletion process is lawful https://www.privacy.org.nz/news-and-publications/commissioner-inquiries/profile-engine-deletion-process-is-lawful/

Examples of complaints to NetSafe involving personal harm

A 13 year old girl was befriended on social media and following a period of grooming was persuaded to upload sexual videos to a Vine account, a service owned by Twitter. The new friend then changed the password for the account and tried to blackmail the child into creating more videos. A worried parent contacted Vine but received only an automated reply. After the parent talked with the school, it was discovered that other students had seen the content. The parent contacted OCEANZ and NetSafe and although accepting they may remain online forever, wanted the videos removed from Vine.

Removing the harmful content from commonly accessed spaces reduces the stress on the victim. Therefore, NetSafe contacted Twitter staff via a US partner. The Vine safety team responded immediately. They removed the videos and reported the offender to the FBI's National Centre for Missing and Exploited Children (NCMEC).

A 16 year-old boy accepted a friend request on Facebook and began messaging what he believed to be a teenage girl. 'She' asked him to send a naked selfie. After he sent the picture, 'she' started to blackmail him to send more photos. He was understandably concerned about would happen with the photo if he did not send more images. He closed down all his social media profiles and contacted NetSafe.

The blackmail and child safety aspects of the case made this incident a Police matter. NetSafe referred the case to the New Zealand Police's OCEANZ unit who made contact with the boy immediately. Also, the fake Facebook page would almost certainly be used to lure other victims. Therefore, NetSafe requested its removal which was immediately actioned by Facebook.

A year 8 student found an Instagram hate page had been created using images copied from her own public profile. The page was reported to the company by school staff and other students. Friends had also tried to defend the girl by adding positive comments to the pages. The school had informed her parents of the incident and the student received assistance to change the settings on her Instagram to make her photos more private. However, the hate pages remained.

This case highlights the valuable networks that rally around the target, and the limitations of those networks. In this case, the friends, school, and family supported the target of the attack - but were unable to have the offending pages removed or deter the offenders. NetSafe contacted Instagram directly and the hate page was removed.

A man received death threats from another online forum user who suggested they had access to guns and knew the complainant's home address. The victim reported he was not sleeping as a result of the threats sent online.

To threaten harm of this type is a breach of section 306 of the NZ Crimes Act 1961 regardless of whether it is made in person or online. NetSafe referred the incident to the Police and advised the man to keep a record of all evidence of the threats made.

A 14 year old boy had shared intimate photos with a 22 year old partner who published them on Facebook after their relationship broke up. The partner removed the photos voluntarily later but threatened to publish them again.

The blackmail and child safety aspects of the case made this incident an urgent Police matter. NetSafe referred the referred to the NZ Police OCEANZ unit for immediate attention.

NetSafe worked with media to increase awareness about blackmail attempts being made using Skype. This was in response to an incident in which New Zealanders were videoed whilst performing sex acts during private chat sessions. The coverage resulted in further reports to NetSafe including this anonymous but typical report:

"I met a lady on Chatroulette and she asked me to Skype her to have some fun. She recorded the call and threatened to send the video to all my Facebook friends if I didn't pay $500 via Western Union. I locked down my Facebook profile so strangers couldn't see my friends any more and was very scared she would carry out the threat. I didn't pay the blackmail but was tempted to. I didn't

A former user of the Tinder dating app was told by a friend that their name and photos were still being used to contact people a year after they had stopped using and deleted the app. Public photos had been copied from their Facebook account to create the fake profile on Tinder. They were worried that the imposter account could cause harm to their personal and professional reputation and that the imposter may be a safety risk to other New Zealand users meeting up face to face. Their attempts to request support from Tinder failed to resolve the situation despite providing evidence of identity.

Fake profiles on dating sites are such a common problem that the service providers seem unable to deal with the volume of reports. The profile was eventually removed but it remained uncertain if the company intervened or the user that created the fake profile removed it.

Following a marriage break up, one ex-partner created a spoof email account for the other. This was created using a free online service and was used to send allegations about personal behaviour to the ex's work colleagues. This resulted in severe mental strain, embarrassment and humiliation in the workplace. The individual targeted tried to get the spoofed email account shut down but could not get a response from the provider. More threats followed to send further emails out.

Incidents where the perpetrator's identity is known, but not easily proved, are common. Evidence of identity is not always required to activate safety responses. NetSafe advised the complainant of this and recommended that the evidence of harassment be taken to Police so that a protection order could be drawn up.

Reports involving a financial loss

Headline figures

In 2014 the total value of direct financial losses reported to NetSafe due to online fraud and scams was nearly $8 million recorded[8] at exactly $7,986,406.37. The largest single reported loss was $1 million. The smallest was 39 cents. The mean average loss for each report was around $9,300. There were 31 losses of more than $50,000 reported.

Online fraud and scams

Investment, romance and upfront payment scams remain the most challenging issues for New Zealanders going online. More than $3.1m was reported lost to various investment scams involving property deals, share trading and betting software. A total of 38 victims contacted NetSafe during 2014 with an average loss suffered of $82,000.

A total of $1.5 million was reported lost by 67 romance scam victims while inheritance scams and other upfront or advanced fee frauds led to losses of $1.2 million. Small businesses were also hit with a variety of challenges over the year and incidents in these three categories involved an average loss of around $23,000.

NetSafe recorded 839 reports related to a range of e-commerce platforms. These included 490 reports of deals going sour on Facebook ‘buy and sell’ pages. An average loss of just over $800 was reported in relation to sellers failing to deliver goods, ‘disappearing’ or purposefully defrauding shoppers.

Computer security

Computer security threats received wide publicity during 2014 (named by some in the media as ‘the year of the data breach’) and 520 incidents were reported to NetSafe. NetSafe recorded 25 cases of direct financial harm caused by ransomware, network intrusions and low-level hacking with the average incident costing $10,700.

[8] Some losses are provided in foreign currencies which are converted to NZ dollars at the time the report is received.

Reports involving financial harm

Upfront payment scam – total loss $5000

I received a message on Facebook from an old friend about her winning a big lottery prize. She said that I should get in touch with the company as I had also won. Because it was from someone I trusted, I thought the message must be real and got in touch with an agent based in America. He asked me to pay the taxes and fees before I could receive the prize and eventually I decided to send the payment but the money never arrived. When I sent him more messages he asked for more payments for customs charges but I was suspicious and phoned my friend. She confirmed that her account had been hacked and that she hadn't sent the original messages about the lottery win. My money couldn't be recovered.

ADVICE:

Be suspicious of any lottery or competition notifications you receive via messaging services including Facebook, text message or email. Website adverts also promote competition prizes using brand names that New Zealanders trust but who are not behind the prize draws. Value your personal information and don't give out lots of details to claim a prize and never pay out fees in advance to claim a big win.If you are suspicious of a message from a friend try to contact then by another method. Strong, unique passwords are an excellent way to prevent your accounts from being compromised online and used by scammers to trick friends and family members.

Employment ‘money mule’ scam – total loss $4600

I was looking for part-time work around my studies and applied for a work from home customer services role that I saw advertised online. The company asked me to submit an application form with lots of personal information and send a scan of my passport and my NZ bank account number. When payments arrived I withdrew cash, keeping a commission and sent the rest overseas via a money transfer company. A couple of days later all the money was taken back out of my account and I was left in debt. I’m also worried my identity will now be used by the criminals.

ADVICE:

Be cautious with your personal information and research a potential employer - just as they would research any job seeker - before you send off your CV. A scan of your driving licence or passport has value for cybercriminals and may be used in other fraudulent activities so think twice before storing and sending ID electronically. Services designed to send money overseas highlight the fact you should only send funds to people you personally know and ‘muling’ funds offshore for a commission can leave you thousands of dollars in debt.

Investment scam - $170K lost

I was contacted by an overseas broker suggesting I could buy shares in a company soon to list on the stock market. They had documents suggesting the floatation was genuine and many shares were being purchased. They also sent me a passport scan for the broker to confirm they were a genuine person and I believed the share offer and the company was real. Once I had invested the money the company disappeared and I can no longer contact them.

ADVICE:

‘Boiler rooms’ have operated for many years targeting investors with such stories by phone and increasingly online. In many cases, they have professional looking websites and smooth talking sales staff who are skilled at sealing a deal with the promise of good returns.

New Zealanders should be suspicious of any unexpected investment offers and always deal with companies authorised to operate in NZ. Check the Financial Service Providers Register before handing over cash (https://www.fma.govt.nz/help-me-invest/risks-involved-in-investing/being-alert-to-scams/checking-the-financial-service-providers-register/) and investigate the ownership of any websites they are sent to. NetSafe has seen complex online account management systems displaying promising balances which are still online long after the company has disappeared and stopped responding to emails and calls.

Small business scam - $76,000 lost

I regularly order items from a Chinese based supplier that my company has used for years and trusts. When an invoice arrived by email with a new bank account number we made the payment and assumed the order had been accepted and goods would soon be dispatched. It was only several weeks later when the supplier questioned why the funds had not arrived that we realised the email had been intercepted and our payment had been made to an account not used by the company. The Chinese company confirmed that their email system had been hacked and the funds had already been withdrawn and could not be recovered.

ADVICE:

Small businesses are the lifeblood of the NZ economy and these types of scams can be hard to recover from when a computer security incident overseas leads to a payment being made to the wrong bank account. If you order from suppliers and a bank account number on an invoice changes make contact with them using a method you can trust - if calling them use the number you have used before, not the phone number shown on the suspect invoice. Email is not a secure communications channel and business owners and staff need training and guidance on how to spot scams, phishing emails and malicious attachments with this knowledge backed up with good computer security policies and tools.

Romance scam - $40,000 lost

I met a new American partner online and although she was based overseas we communicated a lot by email and text and over several months I came to believe we could be together. She wanted help getting her family's possessions transferred from Ireland and I sent money through to help. On the day the possessions were supposed to arrive in the US I got a message saying she had been arrested and requests for help continued to come through. I now realise the money has been lost.

ADVICE:

Romance scammers are good at what they do and can spend months building up trust before they start to ask for small sums of money. Any request for payment via money transfer should set off alarm bells if your new love mentions health problems, family issues or any of a dozen or more excuses. Poor spelling or grammar is an obvious giveaway; so too is a change in style where several scammers may take turns to message you. Over the top confessions of love within days of talking can also be a giveaway.

Computer security incident - $250 lost

I use my computer for freelance design work and was completing a new project when a warning message appeared on my computer screen saying that I had looked at child pornography and NZ Police demanded I pay a $100 fine. A countdown timer suggested I had a limited amount of time to purchase a voucher code before the fine increased. I had done nothing illegal but needed to unlock the computer to hit a work deadline and so paid for and entered a code. After spending $100, nothing happened so I called New Zealand Police who told me it was a scam and to speak with NetSafe. I had to pay more money to have my computer fixed.

ADVICE:

Ransomware - malicious software that infects a computer and potentially encrypts data - has become a growing problem for home internet users and small businesses which may rely on older hardware and have limited resources and knowledge on applying security patches. 'Police' ransomware that uses an authentic looking logo and threats around user behaviour is designed to embarrass or scare the owner into paying a fine or ransom to get access back to their computer or data within. An active approach to software and operating system updates and routinely backing up important data is the best method of preventing fallout from such an infection. Clean up costs connected to the initial security breach can also add to the impact.

Where were requests for support received from?

Whilst data reflects metropolitan population densities, digital challenges have an impact on all communities around the country including two reports made by Chatham Islanders. A geographic location was recorded for 87% of reports made during 2014.

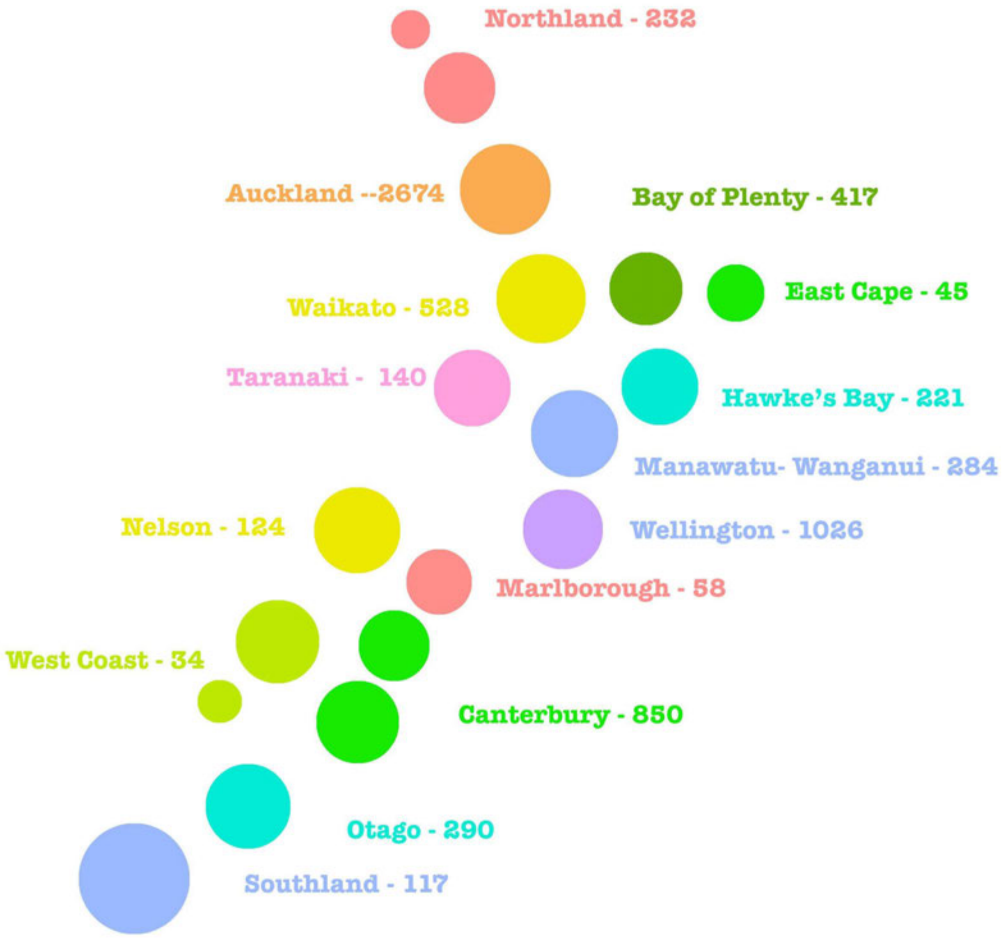


Figure 3 Incident report numbers mapped against 16 New Zealand regions:

NetSafe by numbers

Education Sector

NetSafe handled 340 requests for support from New Zealand educational organisations from early childhood through to tertiary. In total, nearly 13% of all NZ schools contacted NetSafe directly for support in 2014. This does not include schools that accessed online resources or social media. For example, the NetSafe Kit for Schools[9], first released in 2001, is the main framework for building capacity and capability in the education sector around digital challenge and digital citizenship. Nearly 400 school administrators have access to the Kit's online tools for surveying students, staff and the wider community. These enable them to self-assess their current abilities and identify opportunities to strengthen their online safety approach.

In the community

NetSafe delivered 115 training sessions, workshops and conference presentations reaching over 4800 individuals face-to-face across the country. Frequently, NetSafe is asked to work in across a community in coordination with local organisations.

Broadcast and Publishing media

Over 2014 there were 2382 recorded items of NetSafe media coverage reaching a cumulative audience of 26,176,893 people with an advertising space rate of $2,611,487. This is indicative of the interest in issues related to digital challenges and the national dialogue that is already taking place.

A significant number of New Zealanders contact NetSafe directly from an internet search related to their issue or after visiting one of our websites. NetSafe also receives many enquiries via partnerships with community organisations, personal recommendations from friends or through family members attending a face-to-face presentation or workshop. This illustrates how New Zealanders are going online to look for help with the challenges they experience.

[9] http://www.netsafe.org.nz/the-kit/

Trends

What are the patterns that NetSafe identifies from its work supporting people navigating the digital challenges?

Cyber safety challenges

The evolution of the two ‘Ps’ | Pornography and Predators

When internet access became common there was a real concern about the connections it enabled between young people, pornography and predators (the two ‘Ps’). However, it soon became clear that other challenges, such as text and cyber bullying, were more prevalent and the focus shifted. These challenges reflected the technology, connectivity and online services available at the time (early 2000s); homes had dial-up internet speeds, mobile phones could only send SMS texts and social media hadn’t been invented. Wind forward to 2015 and the two P’s have evolved and are making a serious comeback.

Pornography, specifically self-produced pornography, is on the rise. Most people will immediately think of ‘sexting’. The Oxford Dictionary defines sexting as “sending (someone) sexually explicit photographs or messages via mobile phone”[10]. From celebrities to children, everybody seems to be doing it. Once it is produced and shared the story can go bad and, frequently, does. However, what is becoming increasingly clear is that this definition of sexting is too narrow to cover the scope of problematic behaviours reported to NetSafe. It also doesn’t begin to describe the scope of its impact on issues such as gender roles, early sexualisation of young people or its relationship to predatory behaviour.

Where there is risqué content, there’s opportunity for exploitation. Frequently this manifests itself in reports to NetSafe as blackmail. With the threat to release this content hanging over them, an increasing number of people report being coerced into, for example, providing more explicit content.

This predatory behaviour is not confined to adults. We are increasingly seeing young people looking to exploit their peers in this way. Overall, NetSafe is observing a shift that is seeing predatory behaviour increasingly take place in the internet ‘mainstream’.

[10] http://www.oxforddictionaries.com/definition/english/sext

Age restrictions continue to be a counter productive safety tool on social media

The USA's Children's Online Privacy Protection Act (COPPA) sets the age of consent for sharing personal information at 13 years old. This isn't a legal requirement in NZ, but the main social networking sites that New Zealanders use typically require users to be 13 in their terms and conditions.

Young people are using, and will continue to use, these services by lying about their age. This behaviour is often supported by their parents who may support their child to have a positive online experience. This creates a safety challenge. It is not reasonable to expect social media service providers to provide safety support services that cater for younger users if they should not be using a service.

Changes made to the COPPA in 2013 did not substantively change the equation for the social network providers. They were predicated on the belief that social network providers can, and therefore should, enforce age restrictions. At this stage, the regulatory environment in the USA does not encourage social networking services to actively engage younger users on their service, and this is unlikely to change in the short term. This has a flow on impact on New Zealand's young internet internet users.

Increasing use of digital technology in schools brings new challenges

The National Administrative Guideline Number 5(a) states that each Board of Trustees must provide a safe physical and emotional environment for students. Digital technology has increased the difficulty and cost of meeting this standard.

Many threats to student emotional and physical well being in the classroom are initiated outside of the schools' traditional boundaries. Schools are involved in an increasing number of incidents where the activities of students at home or in their own time have an impact on the life of the school. This presents schools with a range of challenges, the first of which is knowing the extent of their power and responsibility to act. They may have to work with parents that are unaware of an incident, or believe that it is the school's responsibility to resolve it.

At the same time, an increasing number of student-owned digital devices are being brought into schools; some as part of the education programme and some as personal items. This proliferation of powerful internet-enabled devices in schools means that teachers are being confronted by a range of new challenges to understand and manage.

Schools' capability to manage these challenges should not be underestimated. They have been actively doing so for over 10 years. However, current accessibility to digital devices and the internet in schools is rapidly increasing, primarily driven by schools recognising the potential benefits to learning and investments in ultrafast broadband for schools. NetSafe is seeing this reflected in the challenges schools are experiencing. Overall, it is becoming clear that schools require increasing support to meet these challenges.

In 2014 the Ministry of Education led the development of a cross-sector cyber bullying prevention group. In 2015 NetSafe is working with the Ministry to broaden this group's remit and create the Online Safety Advisory Group (OSAG). Coinciding with Safer Internet Day 12015, the OSAG is releasing a guide for schools about the safe and responsible use of digital technology in schools. This is a companion to the guidelines for the surrender and retention of property and searches[11] released by the Ministry of Education in February 2014. The guide provides advice for schools on how to manage digital technologies, such as smartphones, under the Education Act 1989. The release of the guide provides a very simple example of an initiative supporting schools create safe digital learning environments for students.

Cyber crime challenges

Under reporting leads to under resourcing

Statistics New Zealand publishes statistics about crime and justice[12] that inform policy decisions such as resourcing policing. These do not distinguish between on and offline offending. An analysis of the statistics for "Fraud, deception and related offences" reveals that since June 1995 the annual number of crimes recorded decreased by 75% to 7,906 ending June 2013. Compare this to the estimated 112,800 New Zealanders[13] that reported being victims of online fraud in 2012.

Before a crime can be recorded the matter needs to come to the attention of police. Crimes most likely to be reported include those that involve insurance claims and those where injuries require medical treatment[14]. In general these conditions do not apply to cyber crimes.

Factors affecting whether a crime is reported to police that, based on NetSafe operational experience, are directly relevant to the reporting of cyber crime include the perceived seriousness of the crime, and a perception of how police would deal with the matter.

In short, under reporting of cyber crime directly results in under resourcing of cyber crime enforcement, that in turn can result in further under reporting.

[11] http://www.minedu.govt.nz/Boards/SupportForBoards/SurrenderAndRetentionOfPropertyAndSearches.aspx

[12] http://www.stats.govt.nz/browse_for_stats/people_and_communities/crime_and_justice.aspx

[13] NZ Stats Household Use of ICT 2012

[14] Crime and Justice, Statistics NZ.

Cyber security challenges

The threat and response are both evolving

The trend of increasing data breaches and other cyber security incidents will continue. The barriers to potential perpetrators continue to reduce. For example, attack toolkits are sophisticated, cheap and relatively easy to use. In 2015, perpetrators will continue to hold the upper hand. After all they only have to be lucky once when seeking to exploit security flaws.

Looking Forward

The eyes of the world will be on New Zealand as it implements the Harmful Digital Communications Bill

Many Governments are considering a regulatory response to online bullying and harassment. New Zealand has developed the HDC Bill which, at the time of writing, is awaiting its second reading in Parliament.

Internationally, the ICT industry is wearying of attempts to regulate online behaviour. Previous attempts have been unworkable, ineffective and expensive. This is primarily because they have generally run counter to the realities of the online world. By contrast, the HDC Bill attempts to construct a regulatory process that aligns with the existing safety processes of the ICT industry. This also means that other countries are looking with great interest at New Zealand's experience.

New Zealand has a reputation for taking a pragmatic and effective approach to online safety. The ICT industry will be hoping the country reinforces that reputation and produces a workable solution that other Governments can replicate. Critically, this requires the HDC Bill to be implemented as a package of measures as envisaged by the Law Commission in its Ministerial Briefing on Harmful Digital Communications[15].

[15] Ministerial Briefing Paper, Harmful Digital Communications: The adequacy of the current sanctions and remedies. Law Commission - Te Aka Matua o te Ture, August 2012

Partners and Activities

NetSafe operates as a multi-stakeholder organisation and has worked with many New Zealand and international partners since 1998. Examples of partnership projects undertaken in 2014 are provided below. For more information on other projects please contact NetSafe directly at SIDreport@netsafe.org.nz

Operating the Online Reporting Button website involves the ongoing support of New Zealand Police, Department of Internal Affairs, the Office of the Privacy Commissioner, Consumer Affairs, Commerce Commission, National Cyber Security Centre, New Zealand Customs Service and Trade Me. Visit the ORB at http://theorb.org.nz

Staying Safe Online

Publication of the *Staying Smart Online* guide with leading online companies including Facebook, Google, Microsoft, Trade Me, Twitter, Yahoo! and YouTube. Sponsorship funding allowed the production of 10,000 print copies and distribution to every New Zealand school. The guide is available from download from www.netsafe.org.nz.

NetSafe and Google worked to develop **the Web Rangers NZ programme** to empower Kiwi teens to campaign for the safe use of the Internet in a creative way. One hundred and forty 14 to 17 year-olds from Auckland to Alexandra took part in workshops around the country where they learned how to build successful public awareness campaigns. See the winning entries at www.netsafe.org.nz/webrangers/.

NetSafe is grateful for the support of all of the **Safer Internet Day 2015** partners. Visit the dedicated website for a summary of the partners particpating on 10 February 2015 at www.netsafe.org.nz/safer-internet-day

NetSafe is grateful for the support of the following organisations:

InternetNZ

MINISTRY OF EDUCATION
Te Tāhuhu o te Mātauranga

Privacy Commissioner
Te Mana Matapono Matatapu

enabling e-Learning

N4L
Network for Learning

PPTA
NEW ZEALAND POST PRIMARY TEACHERS' ASSOCIATION
TE WEHENGARUA

TE TOI TUPU
LEADING LEARNING NETWORK

core
EDUCATION
Tātai Aho Rau

trademe
Where Kiwis Buy and Sell

Real me

NEW ZEALAND PRINCIPALS' FEDERATION
Ngā Tumuaki O Aotearoa

Google

connect
SMART
Protect yourself online
newzealand.govt.nz

The
Cooperative
Bank

MANAAKITIA A TĀTOU TAMARIKI
Children's
Commissioner

vodafone

YAHOO!
NEW ZEALAND

Microsoft

UNESCO
United Nations
Educational, Scientific and
Cultural Organization
New Zealand National
Commission for UNESCO
Te Kōmihana Matua o Aotearoa mō UNESCO

INTERNAL AFFAIRS
Te Tari Taiwhenua

CONSUMER AFFAIRS
MANATŪ KAIHOKOHOKO

COMMERCE
COMMISSION
NEW ZEALAND
Te Komihana Tauhokohoko

NCSC

NEW ZEALAND
CUSTOMS SERVICE
TE MANA ĀRAI O AOTEAROA

Human Rights
Commission
Te Kāhui Tika Tangata

Spark

Youthline
Changing lives.

Citizens
Advice
Bureau

0800
WHAT'S
UP?

THE
PARENTING
PLACE

Australian Government

acma

cyber(smart:)

UK Safer
Internet
Centre
www.saferinternet.org.uk

Family
Online Safety
Institute

INTERNATIONAL ASSOCIATION OF INTERNET HOTLINES
INHOPE