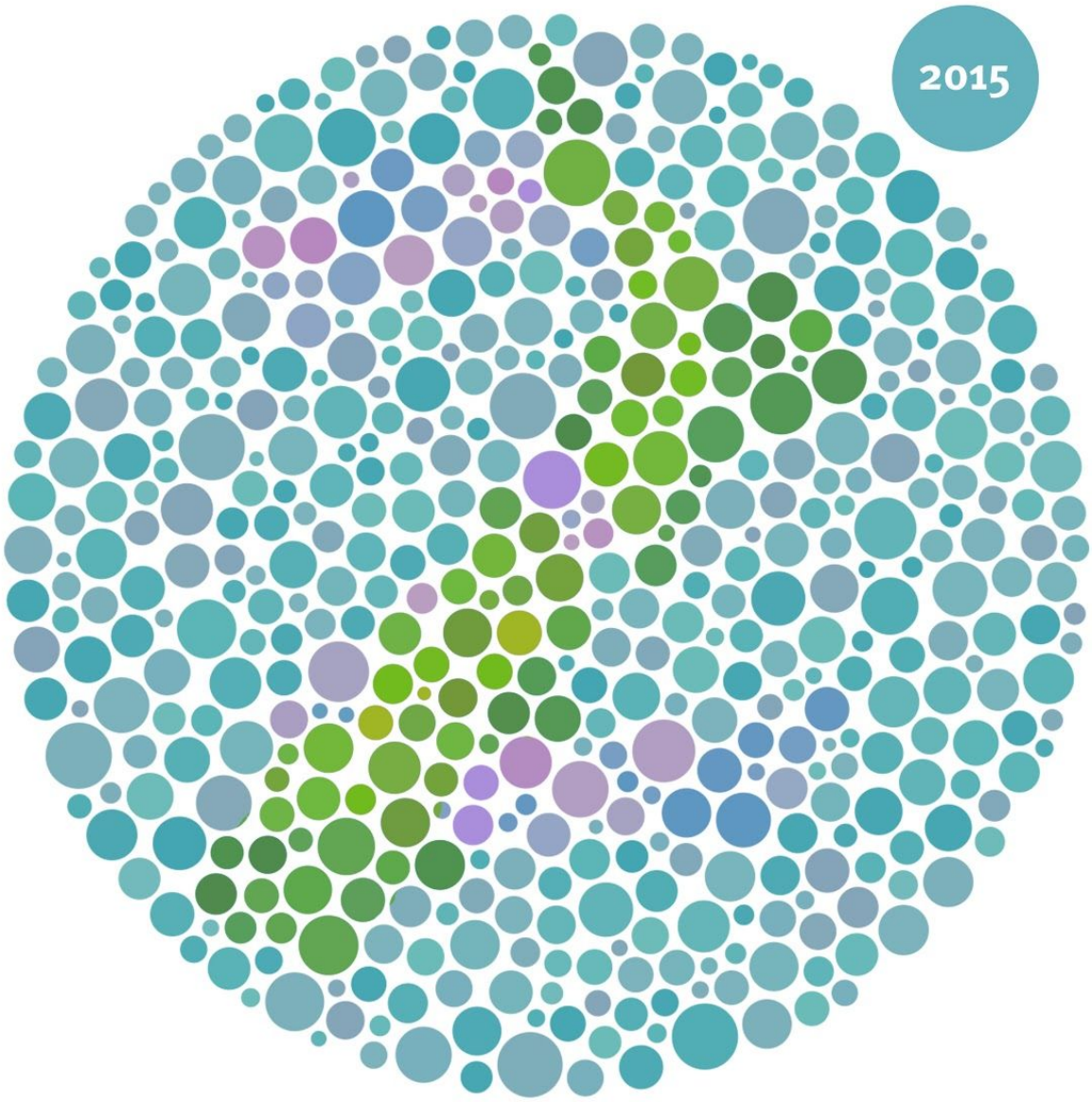
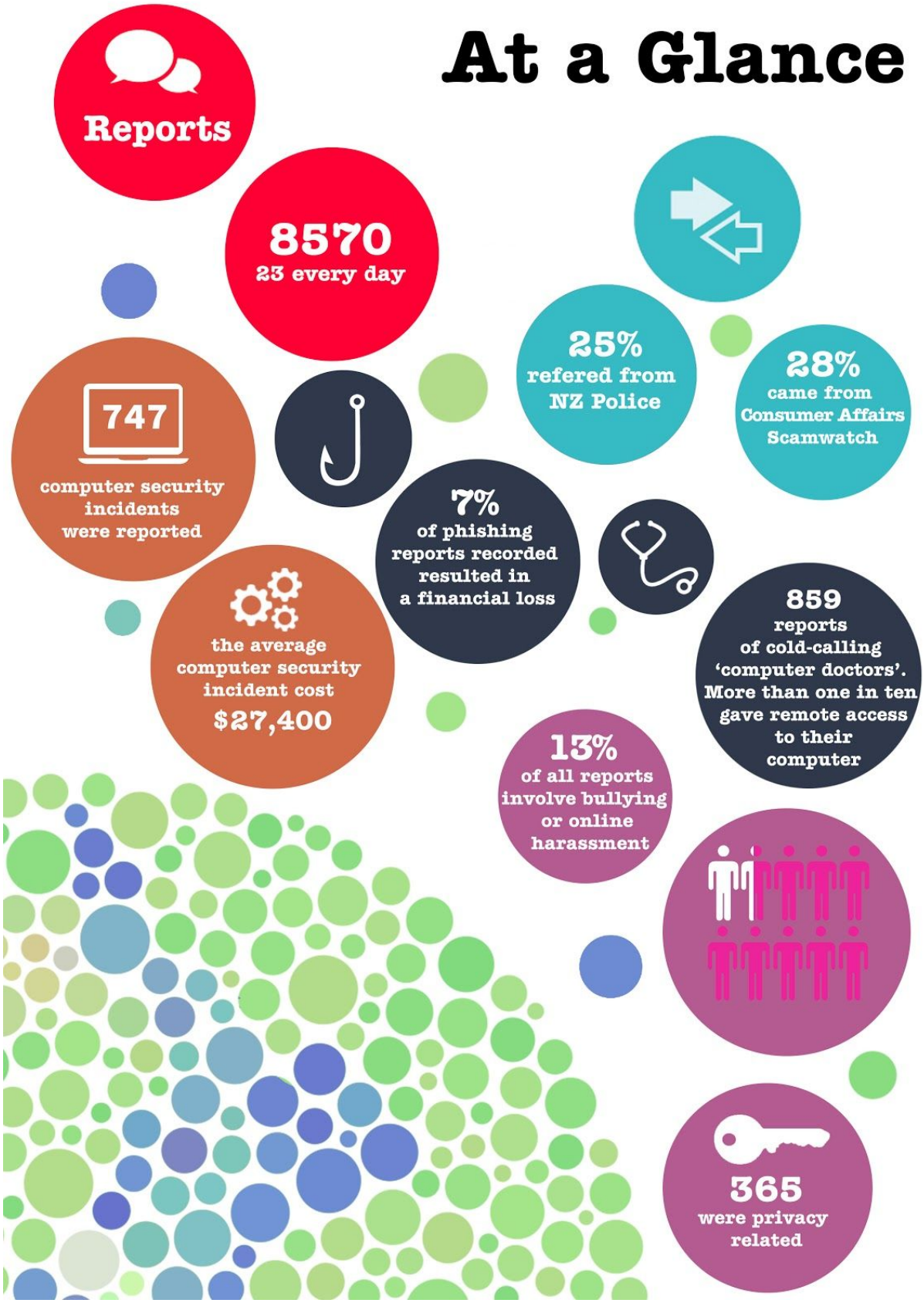
Digital challenge and New Zealanders

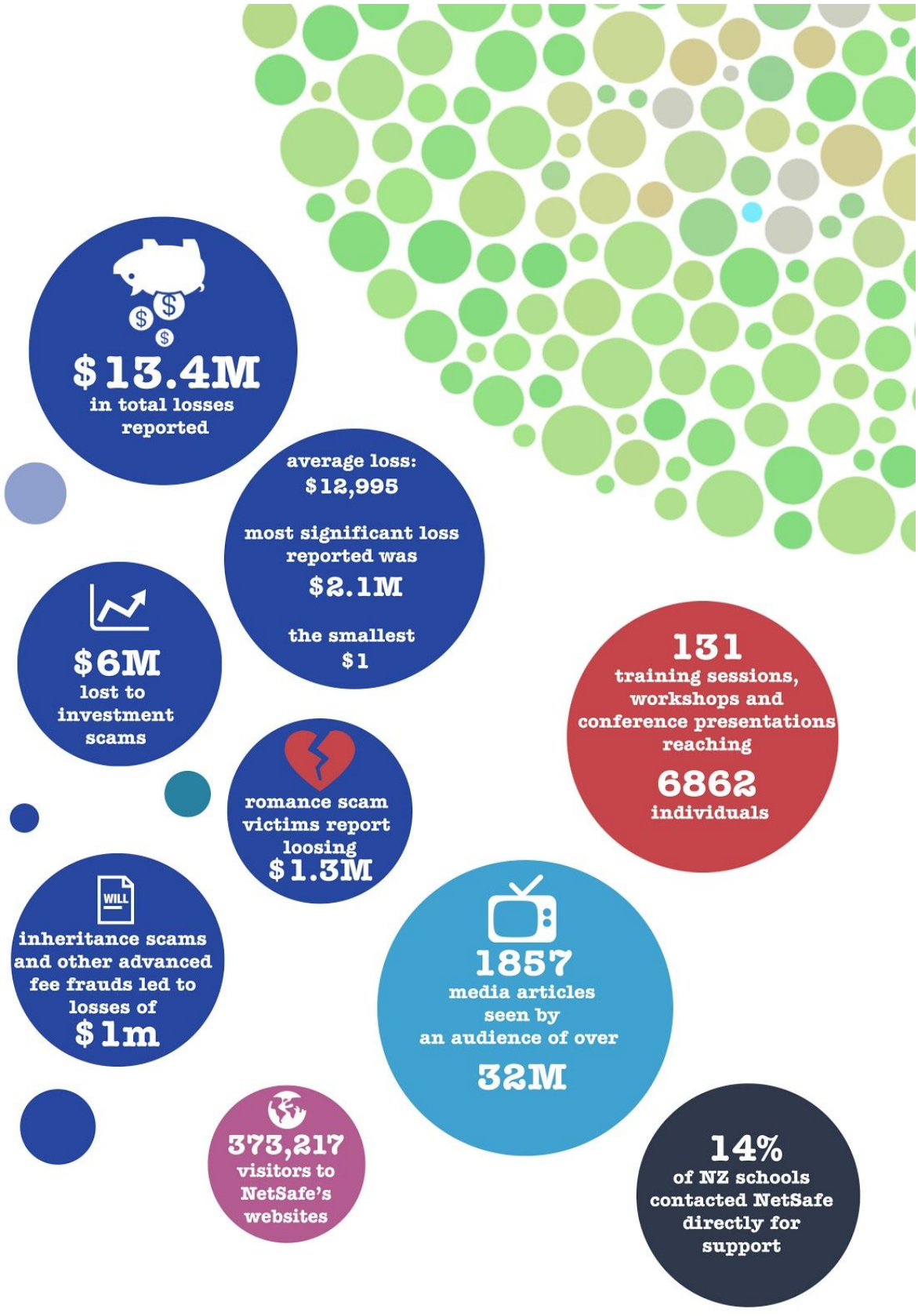
A focus on the incident reports and queries made to NetSafe in 2015



A NetSafe Report for Safer Internet Day | 9 February 2016

At a Glance


Reports
8570
23 every day
747
computer security incidents were reported
25%
refered from NZ Police
28%
came from Consumer Affairs Scamwatch
7%
of phishing reports recorded resulted in a financial loss
the average computer security incident cost
$27,400
859
reports of cold-calling 'computer doctors'. More than one in ten gave remote access to their computer
13%
of all reports involve bullying or online harassment
365
were privacy related


$13.4M
in total losses reported
average loss:
$12,995
most significant loss reported was
$2.1M
the smallest
$1
$6M
lost to investment scams
131
training sessions, workshops and conference presentations reaching
6862
individuals
romance scam victims report loosing
$1.3M
WILL
inheritance scams and other advanced fee frauds led to losses of
$1m
1857
media articles seen by an audience of over
32M
373,217
visitors to NetSafe's websites
14%
of NZ schools contacted NetSafe directly for support

Introduction

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.

This report is the second annual report released on Safer Internet Day. It draws from the over 8500 requests for help and incident reports received by NetSafe in 2015 and provides a snapshot of the of the digital challenges that New Zealanders face.

NetSafe produces this report as a contribution to the ongoing national dialogue about the digital challenges impacting New Zealand Internet users.

Creating a better internet through partnerships

This report is released for Safer Internet Day 2016. Safer Internet Day is an annual event celebrated worldwide to encourage the safe and positive use of the internet and digital technologies.

Online safety is often thought about as primarily an issue for young people. While it is true that young people are disproportionately affected by certain digital challenges, such as cyberbullying, every New Zealander and New Zealand organisation can experience challenge online. These include scams, hacking, privacy breaches and harmful digital communications.

As a country New Zealand needs to continue to develop appropriate responses to all such challenges. As can be seen in this report, there are direct personal and financial consequences to not doing so. Further, every successful cyber security breach, act of cyber crime or negative online safety event impacts people's confidence in the technology they use every day.

As the volume of online activity grows, so too does the challenge of creating a safer more secure online environment. Rising to this challenge requires the collective efforts of government, business, NGOs. Few countries could claim to have a more productive and cooperative multi-stakeholder online safety community than New Zealand. It is in that spirit that this community comes together to celebrate Safer Internet Day.

Using the data

This report is part of NetSafe's ongoing programme to share data that can be used to improve the national response to digital challenges. If you are interested in receiving more regular updates from NetSafe we recommend subscribing to the monthly newsletter (http://www.netsafe.org.nz/computer-security-email-newsletter/) and joining us on Facebook www.facebook.co.nz/netsafe and twitter @netsafenz

Looking ahead to 2016

In 2015 the Harmful Digital Communications Act was passed into law in response to the issue of online abuse and harassment and a revised national strategy for cyber security was released. Looking ahead to 2016 these provide the basis for a range of initiatives to be put in place that will be of direct assistance to all of New Zealand's internet users.

However, at the same time online challenges will continue to evolve and increase in both frequency and complexity requiring continued collective effort. We hope that the spirit of Safer Internet Day will continue throughout the year and that the community will face those challenges with confidence. Playing its part, NetSafe will ensure New Zealanders have access to high quality online safety support and information as well as working with any organisation with a shared interest in creating a safer and more secure internet.

Ngā mihi nui

Martin Cocker
Executive Director

2015, safer and more secure than 2014?

NetSafe is often asked if particular digital challenges are on the rise. There are a range of reasons why it is difficult to answer that question definitively. NetSafe receives only a fraction of the total number of online challenges that New Zealanders experience each year. As such, the data in this report is representative of the experience of many more New Zealanders. Further, people have different motivations for reporting an incident to us. Many choose not to report the challenges they have experienced, again for a range of valid reasons.

Simply put, data derived from reports made to NetSafe can only provide a snapshot of the challenges that New Zealanders face. It is sufficient to draw broad conclusions and shape NetSafe's own work to reduce online harms.

Research tells us that as more people go online for longer that the frequency of digital challenge they experience will go up. This continues to be reflected in the fact that the volume of reports NetSafe receives goes up year on year. In 2015 we received 8570 requests for advice or support an increase of 6% on 2014.

Reporting rates provide an indication of possible trends in the prevalence of particular types of online challenge. So while overall the rates of reports made to Netsafe went up in 2015, there were some interesting changes from 2014. For example, the increase in average financial loss due to online fraud and crime jumped from $9,300 in 2014 to $13,000 in 2015. It should be remembered that the numbers for financial loss do not include incidental losses incurred when recovering from a problem. Neither does it reflect other, non-financial, types of harms that people can experience when they have been targeted, for example, by bullying and online harassment across New Zealand. The impact of this emotional harm is much more difficult to quantify. Figures comparing the change in average financial loss to scams in NetSafe's 2014 and 2015 data are provided in the Appendix.

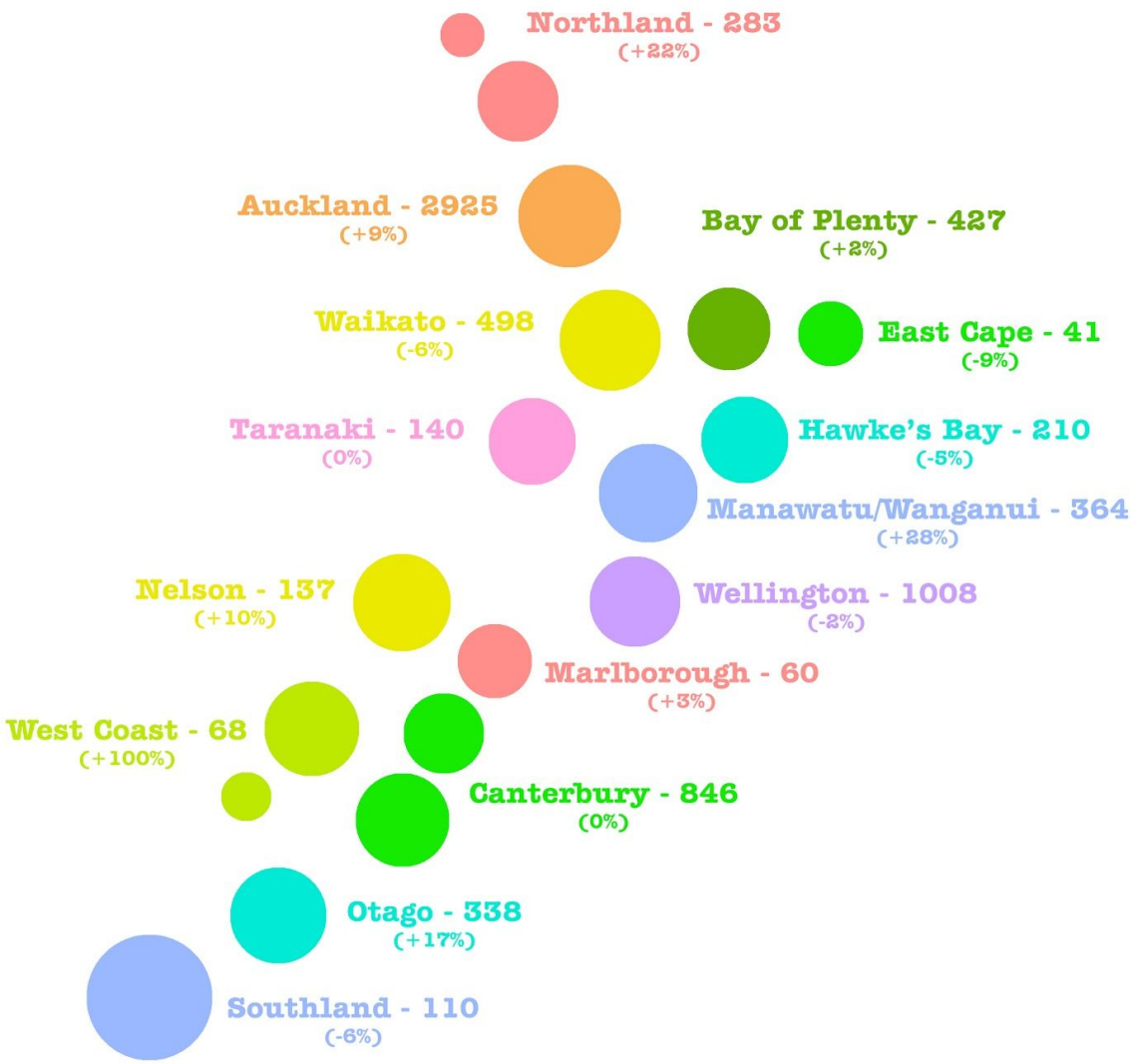
It isn't just overall reporting that continues to increase. There is increased demand across all NetSafe's services. While this may be, at least in part, due to an increasing awareness of NetSafe and its services, it also suggests that the levels of digital challenge New Zealanders are experiencing is increasing bringing an increased demand for information and support.

Headline figures comparing NetSafe's 2014 and 2015 data are provided in the Appendix.

Where did requests for support come from?

- More than half of reports come from metropolitan centres
- Significant rise in reports from Northland, Manawatu and West Coast residents since 2014 *although volumes remain low*

Figure: 2015 Incident report numbers mapped against 16 New Zealand regions with + or -% change from 2014



What were the significant challenges in 2015?

The evolution of business focused scams

Business Email Compromise

In 2014, the majority of reports made by business owners concerned traditional scams such as fake invoices and low level frauds targeting grant applications and other business related activities.

These types of scams continued to be reported in 2015 with the highest profile case involving a German based directory offer that was delivered en masse via the international postal system. However, there was an increasing incidence of businesses reporting scams specifically targeting staff members to extract financial payments via email. This is called Business Email Compromise [1](BEC).

BEC can take 3 standard forms and can impact anywhere along the supply chain. In the first form, genuine suppliers, often overseas in China or Vietnam, can find their email systems or wider computer networks infiltrated and invoices modified with alternate payment instructions.

In the second form, executive level email accounts are compromised or simply spoofed to send urgent or secretive payment requests to finance staff. For example, NetSafe received several reports where businesses had received scam emails requesting payments seemingly legitimate invoice payments. These had been sent from domain names that look similar to the business's purchased specifically to target it. Typically the email accurately identifies relationships between executive level and operational finance staff making the payment requests look very plausible. This underscores the need for staff to be trained to identify suspect instructions and processes to check payments before they are made or better still, to stop the emails arriving in the first place.

In the third form, the company's own systems are compromised. Typically this involves exploiting unpatched software, weak passwords or outdated computer security practices. Suspicious emails often include links to websites hosting malware or carrying malicious .pdf, .jar and .zip payloads. Emails are then sent out to existing customers with modified invoices that directs payment to a new account that is often managed by an unwitting New Zealander recruited as a 'money mule' to send funds offshore.

[1] https://www.netsafe.org.nz/identifying-and-preventing-business-email-compromise/

NetSafe recorded numerous reports of BEC in 2015. A dozen were successful and almost half a million dollars was lost.

Websites under attack

In 2015 businesses increasingly found their websites under attack with reports of DDoS extortion demands, defacement by 'Middle Eastern' hacking gangs or the creation of cloned sites where content including staff profiles is used to recruit money mules or perpetrate identity theft overseas. In some cases, popular brands were subject to the creation of fake online ordering sites where customer could be targeted for personal information and/or payment card details.

One small business owner reported that their website database had been hacked with scam emails sent to all customers resulting in customers losing money. The hacker demanded a ransom to not publish customer data online. In some cases, cyber criminals simply use website vulnerabilities for their own benefit, leaving staff to clean up associated mess. At the start of 2015 NetSafe recorded multiple reports of New Zealand charity websites being used to validate stolen credit cards from overseas with hundreds of payments submitted and accounts staff spending days to sort out legitimate and fraudulent payments with their banks and merchant providers.

The global popularity of free, open source software to design and build low cost websites has resulted in some content management systems becoming common targets for automated attacks. Towards the end of the year, there was an increase in NZ business websites being used to host both phishing pages and to drop exploit kits on unsuspecting visitors or those with unpatched software. Businesses of every size should ensure they use suppliers who are aware of common web application exploits and that they budget for ongoing maintenance and security updates once a site has 'gone live'.

Attribution and authentication: It’s complicated

Doctors’ house calls cause financial headache

For the average internet user, identifying signs of suspicious online situations became more complicated in 2015. This is because of the increasingly 'rapid hit' nature of scam sites that set up to fleece victims as fast as possible before being shut down. Increasingly, overseas individuals looked to NetSafe as a New Zealand organisation for assistance with situations they believed involved New Zealand companies or operators.

Cybercrime operators can register international companies, buy ‘quick to migrate’ but ‘hard to locate’ VoIP-based phone services and hide behind anonymous domains purchased, registered and hosted in three separate physical locations.

For example, the number of reports of the ongoing 'PC Doctor' scam[2] made to NetSafe almost tripled in 2015 (from 313 to 859 reports) with associated losses quadrupling from $26,584 to $103,944. And this is likely to be just the tip of the iceberg.

Caller ID for these operators displayed an incoming number that theoretically traced back to countries as far afield as Egypt, India, Romania, Australia, the Philippines and the US. Other victims reported a browser pop-up requesting you call an NZ 0800 number for virus removal that clearly connected to an overseas call centre.

Identifying those behind cyber incidents is notoriously difficult. For example, in the attack against Sony Pictures[3] in late 2014 the US government threw enormous resources in to investigate claimed North Korean involvement.

To set up a PC Doctor scam is simple. Very little cost is involved in calling thousands of potential victims compared to the rewards, and there is little chance of them being identified. In 2015, reports to NetSafe said the callers claimed they were from trusted local and international organisations including Windows Security, Microsoft Support, Spark, Telecom, Chorus, Norton, Sky, the NZ Cyber Crime Centre and NZ Department of Prime Minister and Cabinet. In the first weeks of 2016, the National Cyber Security Centre issued a warning[4] that callers were now identifying themselves as NCSC staff.

Reasons the ‘PC Doctor’ gave for calling in 2015 typically included requests to clean up viruses and other malware. Many took advantage of the release of Windows 10 to suggest they could help with the upgrade or give guidance on the new product and suitability of the PC. With the rollout of Windows 10 mid-year, NetSafe worked with Microsoft NZ to highlight this ongoing scam and the rise in incident volumes and dollar losses could reflect this high profile awareness raising campaign.

---

[2] https://www.netsafe.org.nz/can-i-trust-cold-calling-pc-technical-support-companies/

[3] https://en.wikipedia.org/wiki/Sony_Pictures_Entertainment_hack

[4] http://ncsc.govt.nz/newsroom/ncsc-name-used-in-new-twist-on-telephone-scam/

Investing in the future… of scammers' profits

The almost doubling of investment scam losses in 2015 (from $3.1m to $6m) also highlights the complexity and cross border nature of cybercrime. Many operators state they are based in financial centres such as Hong Kong or London. Professional looking websites with account management functionality, glossy promotional materials and smooth talking sales staff were increasingly effective selling fake exchange and currency trading services or high growth shares in future boom sectors such as virtual reality or graphene.

In some cases, firms claimed to be based in, and regulated from New Zealand, proudly displaying FSPR registration numbers, listing 09 telephone numbers and CBD addresses. NetSafe worked with FMA staff in 2015 to address this ongoing issue and the organisation is now an active ORB reporting partner allowing NetSafe to triage incidents to add to its report data.

My precious data

As individual internet users we are saving an increasing amount of data online across multiple services. Any form of data or document stored electronically can have value and be easily tradeable or used once an account has been compromised.

Email accounts were increasingly targeted in 2015 and used to scam or send spam to contacts or to gain access to stored copies of scanners driving licences or passports. Airpoints accounts were also targeted for their intrinsic value. Login details for any service that has a credit card linked to it. It can be used to rapidly purchase advertising and promote apps, games or pages for third parties with the victim often unaware of what has happened.

Online Trading Troubles

In 2015, NetSafe received 840 online trading complaints with 540 victims reported having lost money to a variety of websites, social media 'buy and sell' pages and online auction sellers. We noted an increase the use of recently purchased .nz domain names where registrant information couldn't be verified making it hard to track perpetrators of scams. The average sum lost was $773, slightly down on the $801 figure from 2014.

Common items to experience problems when trading included second hand mobile phones. These often arrive 'bricked' (already reported stolen and blocked), sports shoes and electronic goods. Health supplements also remained a particular favourite for scammers. In 2015, many people agreeing to a free or low cost online trial offer found their credit

card charged for an ongoing monthly subscription service which often prove very difficult to get out of.

Analysis of reports made to NetSafe over the year confirms that it remains difficult for online shoppers to discern a trustworthy online only retailer. When rogue sites open for business complaints tend to 'spike'. The sites will then just shut down, all within a time frame of as little as 30 days.

Top targets for Phishing Scams

NetSafe recorded a significant rise in email based threats over 2015, including phishing, spearphishing, whaling (targeting one big 'phish') and various forms of business email compromise.

Criminals continue to target big brands that New Zealanders know, use and trust. In 2015, more than a quarter (26%) of phishing attempts reported to NetSafe targeted the five big NZ banks. In light of recent fake mobile banking websites created and marketed with associated SMiShing[5] campaigns, New Zealanders should remain alert to spoofed requests to part with their banking logins.

Personal harm

Online aggression

NetSafe recorded 931 personal harm incidents in 2015. These range from cases involving a single incident of online aggression (e.g. involving threats or comments traded on a variety of popular social media platforms) through to significant and ongoing campaigns of online harassment.

In last 10 years NetSafe has established strong working relationships with many of the established online content hosts. In 2015 NetSafe made requests to hosts for problematic content to be removed in 10% of all cases it received. On average, nearly 9 in 10 requests to remove content were successful. This is due to NetSafe's operational experience and trusted two way relationships with these commercial providers. Although many popular platforms are based overseas it should be noted that typically these organisations take the safety of their users seriously. NetSafe acts as a local point of reference for individuals experiencing harm who may struggle to navigate existing reporting channels.

---

[5] SMiShing is short for SMS phishing. It is a security attack in which the user is tricked into downloading a Trojan horse, virus or other malware onto his cellular phone or other mobile device.

Getting naked online

The creation and sharing of self-generated pornographic imagery, often termed sexting, has increasingly become normalised by people of all ages. NetSafe recorded more than 60 cases in 2015 where the sharing of sexual imagery or online sexual activity, often live over webcam, had led to blackmail or 'sextortion' demands being made.

In many cases, the perpetrators were overseas and part of an organised gang looking to extract payment by harassing, embarrassing or threatening to share the images or footage of the victim with friends, family and colleagues or by simply publishing to a free video content hosting platform. Some victims paid up to $1500 to the blackmailers, but in many cases this only served to create more demands for money. Some 'revenge porn' situations had developed after a relationship breakup where the other party was known and residing in New Zealand.

This sextortion trend continued in 2015 with the widely reported breach of the Ashley Madison database. This was believed to have exposed the personal details of more than 100,000 Kiwi users. NetSafe received many reports from concerned users, and some not so concerned, about the implications of the release of this data that they had provided in the belief it would be kept secure.

Resolving such cases is becoming increasingly complex due to the number of countries involved each with their laws and regulations. In 2015, two example cases highlight this issue. First, a Swedish resident reported ongoing online harassment by a New Zealand resident using an online service hosted in America. In the second case, a New Zealand teenager was subject to serious harassment and abuse by a Danish resident who utilised online services based in the US and in less well regulated countries to post and publish offensive material.

Looking Forward

Big questions for 2016

Industry and Government: Divided or united?

While everybody agrees that creating a safer more secure online environment requires a multi-stakeholder approach, there is a split in opinion on the best ways to achieve that goal. Governments have been increasingly using their traditional regulatory powers, while industry have voiced a strong preference for self-regulation and industry-led solutions.

Internationally, revelations of government agencies undertaking mass surveillance created a serious rift and led to many ICT companies encrypting customer communications by default.

In New Zealand, NetSafe is hopeful that the implementation of the HDC Approved Agency will create a far more collaborative environment for dealing with online abuse and harassment.

An effective response to young people and pornography?

It has long been known that the lack of effective age verification systems on the internet has been enabling children to easily access pornography. Arguments that young people have always found ways to access pornography have given way to a realisation that the internet has fundamentally changed that equation. Explicit content is now more easily accessible to young children who lack the maturity required to view it without negative consequences. This applies to violent as well as sexual pornographic content.

In response, the UK government has regulated ISPs and now requires them to turn internet filtering on by default (it can be turned off at the request of customers). Given that ubiquitous internet access decreases the effectiveness of home-based filtering, ubiquitous (or near ubiquitous) filtering would seem to be an obvious solution. Filtering is most effective for younger users - where the harm from viewing this content is highest. However, filtering is not as effective a solution as many parents would hope. It certainly doesn't prevent more direct sharing of content between users, and would have little impact on the generation and sharing of self-made pornography.

Like 'parental controls' software, filtering is a first generation safety tool. The focus of online safety has moved from 'protection' to 'preparation' by which the emphasis is

shifted from interventions based on protective strategies (such as filtering and monitoring software) towards those that promote healthy development of online behaviours. The nature of the online environment is such that risks cannot be entirely prevented, and so we must ensure we (and our children) are prepared for them.

NetSafe would like to see the development of technologies that recognise the reality of the online world and focus on preparation rather than prevention as their key safety tools. Technologies that assist parents to be parents, rather than try to replace parenting.

Online safety and security in schools: Keeping pace with the rate of technology adoption?

Increasingly learning in schools includes exciting digital initiatives from BYOD classrooms to online portals for engaging parents directly in children's learning.

Educators are faced with a double challenge of integrating these technologies in a way that benefits education and maintains the safety of children and their data online. Parents that are struggling with managing their own children's online lives will sympathise with educators managing an entire classroom of children.

Creating a safe online environment for staff and students is an entirely more complex proposition today than it was ten years ago. The increased volume and complexity of online activity means that the “policies plus filtering” approach to safety in inadequate.

Online safety requires a coordinated effort between the school and its parent community. We encourage schools to talk to their parents, and parents to talk to their schools about how they can jointly increase students online safety skills and knowledge.

A starting point for engaging with students, parents, family and whānau is to discuss how the school and its community envisage digital technology being used in the classroom and beyond. Other ideas include involving the community in discussions and decisions around online safety and digital citizenship. For example:

- implementing an online safety or digital citizenship committee
- creating a programme of training for staff , students and the community training to build whole school digital capability, or
- creating opportunities for students to share their understanding of digital technology and challenges with adults and their peers.

Emerging in 2016

NZ Computer Emergency Response Team (CERT)

The 2015 NZ Cyber Security Strategy action plan included the establishment of a CERT. It is envisaged that a national Computer Emergency Response Team will bring increased coordination and capacity into the NZ Cyber Security equation.

Harmful Digital Communications (HDC) Act civil process

The HDC Act passed through the NZ Parliament in July 2015. At that point, the criminal provisions were enacted, but the civil processes have been waiting for the establishment of the Approved Agency. That agency should be up and running in 2016 providing New Zealanders dealing with online harassment and abuse access to better support.

#Trending: Predictions for 2016

Converging challenges

The lines between cyber security, cybercrime, and cyber safety challenges will continue to blur. Many single online incidents will include technical, behavioral, and criminal components requiring the intervention and assistance of a variety of multiple specialist services. We expect demand for NetSafe's assistance in helping consumers and families unravel the complexities of these events to continue to increase.

Cyber Crime

2015 saw marked increases in cybercrime targeting higher value targets such as businesses and investors and we expect to see this continue in 2016. Information made public through data breaches and via public sources enables criminals to construct more specific and targeted scams.

CIO Magazine[6] describes the combination of the surge in compliance costs to deal with the uptick in regulatory requirements and the relentless advances in technology against a backdrop of under investment in security departments as creating a "perfect storm" for cyber crime in 2016.

[6] http://bit.ly/CIO-magazine

Cyber Safety

The rise in self-made sexual content continued in 2015, and there is no reason to expect this not to continue into 2016. As taking and sending user generated sexual content becomes more normative, it creates more opportunities for predatory adults.

The issue of online radicalisation has been gaining traction and publicity thanks to the online efforts of groups like ISIS/Daesh. While those specific groups might not effectively reach New Zealanders, other criminal groups will learn from their tactics. Expect to see more traditional gangs and criminal groups embracing online marketing techniques in the near future.

The American Academy of Pediatrics announced it was reviewing its screen time advice that has stood for almost 15 years. The “no screen time for under two, and two hours for children older than two” has formed the basis for many parents screen time rules. The new advice is that it is not how long they are online, but what they are doing online that matters. This more nuanced approach creates challenges for online safety educators and parents who liked the two hour limit as a simple and enforceable rule.

Cyber Security

The rush to mobility and integrating the ‘internet of things’ (iot) picked up pace in 2015. There are fears that hurriedly developed new products and services rushed into the market will not have been properly secured. Under this scenario, the attack surface for organisations and individuals could quickly become unmanageable. Expect to see more cyber security attacks through devices not traditionally thought of as part of the ICT infrastructure like watches, televisions, and security systems.

Appendix | Change in report headline report volumes

Total online challenges reported to NetSafe

	2015	2014	Change (+/-)
Incidents	8570	8121	+6%

Total financial losses reported to NetSafe

	2015	2014	Change (+/-)
Financial Losses ($)	$13,445,660	$7,986,406	+68%

Presentations and workshops to audiences

	2015	2014	Change (+/-)
Events	131	115	+14%
Audience	6862	4858	+41%

Publishing and broadcast media coverage involving NetSafe

	2015	2014	Change (+/-)
Total Audience Reached	32.2m	26.2m	+23%
ASR ($ Value)	$4m	$2.6	+52%

Total cases reported involving cyberbullying, online aggression or harassment

	2015	2014	Change (+/-)
Total reports	931	921	+1%

Appendix | Change in average financial loss to scams

Category	2014 Avg loss	2015 Avg loss	% change in avg loss
Investment scams	$82,002	$158,519	93%
Online trading	$801	$2,882*	260%
Dating and romance scams	$23,411	$22,789	-3%
Upfront payment scams	$23,979	$17,036	-29%
Computer security	$10,689	$27,373	156%
Small business	$22,521	$13,547	-40%
Banking and phishing	$1,632	$7,493	359%
Lottery and competition	$6,952	$11,501	65%
Computer virus scams	$1,022	$1,732	69%
Employment scams	$9,064	$5,082	-44%
Account compromised	$3,727	$1,542	-59%
Flatmate and rental	$1,252	$1,497	20%
Holiday and travel scams	$5,457	$2,160	-60%
Door to door scams	$1,367	$483	-65%
Health and medical scams	$2,798	$188	-93%
Charity scams	$3,742	$0	-100%

*Skewed up by one large loss