IT'S HOW
WE CONNECT

ADDRESSING THE CYBER SAFETY CHALLENGE:

from risk to resilience

July 2014

WHY WE NEED THIS REPORT

Almost 90% of Australians use the internet and more than three quarters of Australians use it more than once a day.

As Australia's leading provider of internet services, Telstra commissioned this report to explore the unique behaviours and risks that face children, young people, adults, seniors and parents in their online engagements. This report identifies the most effective cyber safety strategies to specifically address each age cohort. In recognition of the growing role technology plays in all of our lives, Telstra welcomes this substantial contribution to the public policy arena.

KEY FINDINGS

1. Cyber safety is not limited to preventing cyberbullying or protecting children from online predators. Cyber safety includes minimising the risks of everyone's exposure to: fraud, privacy breaches in credentialing, identity theft, malware, phishing and scams through to internet and device addiction, violent and sexually explicit content, security-compromised online gaming activities and 'sextortion' (extortion involving digital sexual imagery and distribution).
2. One of the most effective ways to be cyber safe is to be digitally literate. Digital literacy enables us to: navigate technology and adjust privacy settings, judge the quality and reliability of online information, and, understand the social norms that apply in online settings.
3. To date, most cyber safety initiatives have focussed on protecting children and young people but have largely failed to address other vulnerable groups including parents, adults, those over aged over 65 and small to medium enterprises (SMEs).
4. Those aged over 65 are commonly the least technologically literate and are often asset rich and therefore particularly appealing targets for those who engage in fraud, identity theft and dating scams.
5. While adults are active users of new communications technologies in Australian workplaces they are mostly computer literate but are not necessarily internet literate due to exposure to online technologies and applications often coming relatively late in their careers.
6. Many parents feel under-equipped to address the numerous and often complex safety issues their children might face online. 91% of parents claim they are aware of their children's mobile phone and online usage, however teenagers overwhelmingly claim that this is not the case.
7. While young people aged 12–17 do not readily distinguish between 'online' and 'offline' activities, they often hold a lot of expert knowledge about new technologies. This makes young people the ideal candidates to transfer knowledge between generations to increase the rates of digital literacy across all age groups.
8. Many SMEs struggle to stay abreast of technological change, often due to limited time or financial/human resources, and find it challenging to move out of 'self preservation' mode when it comes to managing online risks.
9. New technological developments have accelerated our exposure to risk as a consequence of our increased levels and frequency of online engagement. These trends include:
    - user generated content and content sharing platforms;
    - the uptake of mobile technologies and, in particular the adoption of smartphones;
    - cloud computing;
    - platform integration and single sign-on mechanisms; and
    - the rise of GPS and location based services.
10. We learn best by doing rather than by being told. A hands-on approach to learning cyber safety strategies is warranted and some exposure to risk is necessary to improve digital literacy. Increasing the rate of digital literacy and taking account the differing needs of all age groups is the best way to maximise cyber safety – as the risks and benefits of digital participation go hand in hand.

EXECUTIVE SUMMARY

As digital technologies become further integrated into the everyday lives of Australians, users are potentially exposed to greater risks. However, the risks and benefits of digital participation go hand in hand. The challenge, therefore, is to support users to minimise the risks without limiting their digital participation and their capacity to derive the full benefits of connectivity. If Australians are to benefit as either consumers or providers of online services and products in the e-commerce environment, consumer safety and trust need to be improved.

Technology trends and cyber safety

Cyber safety needs to be considered against a transforming backdrop of technology trends, products and practices. While the rise of social media has tended to dominate recent debate and developments in cyber safety, particularly in relation to young people, a range of other trends is also shaping how users engage online, the risks they potentially face in the new media landscape, and the strategies used to address them.

These trends include the rise of user generated content and content sharing platforms; the uptake of mobile technologies and, in particular, the adoption of smartphones; cloud computing; platform integration and single sign-on mechanisms; and the rise of GPS and location based services.

Keep risk in perspective – exposure to risk does not equate to harm, and messaging needs to include the benefits of connectivity

Strategies to address cyber safety

Given that technology will continue to become ever more integrated into everyday life, it is important that cyber safety strategies are flexible and adaptable enough to respond to new opportunities and challenges as they emerge. Effective cyber safety strategies will:

- Address the needs of populations neglected by current policies and programs
- Foster a strengths-based approach with balanced public debate about the opportunities and risks of digital engagement, enabling users to make informed decisions
- Acknowledge that engaging with technology will be a lifelong pursuit
- Keep risk in perspective – exposure to risk does not equate to harm, and messaging needs to include the benefits of connectivity
- Start with the user – the best programs, policies and products are user-centred and actionable
- Recognise the relationship between 'online' and 'offline'
- Ensure approaches are flexible and responsive to market and technology trends
- Undertake research that produces high quality data as new trends and practices emerge
- Build consumer confidence – for industry, trust in brand is critical
- Support active responsibility – tools are just one aspect of cyber safety
- Foster industry, government and not-for-profit organisation collaboration
- Broaden the focus from awareness-raising to long term behaviour change.

Population challenges

A range of demographic factors, including age, impact how users engage with technology. The variation in online activities, combined with different levels of digital literacy, can mean that different age groups are exposed to different risks.

Children (0–11 years)

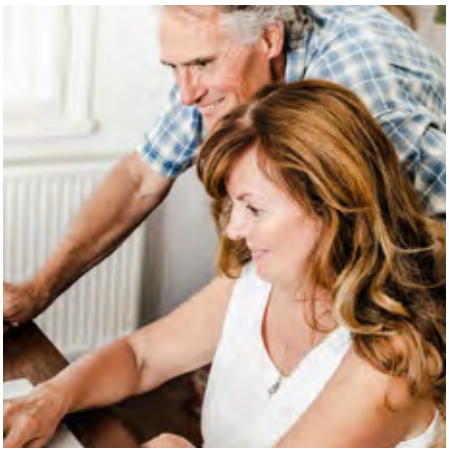
- Australian children are among the youngest first time technology users and many access the internet on a daily basis
- Some exposure to risk is necessary for children to develop digital literacy and resilience
- Children who are most at risk offline are most at risk online
- Children can be exposed to a range of risks, including cyberbullying, online predation, contact with strangers, identity theft and malware
- Children hone their online skills more effectively through exploration and frequency of use rather than through formal training
- Children's online safety may be enhanced by better equipping parents

Young people (12–17 years)

- Predominantly use the internet to socialise with friends, as a source of entertainment and amusement, and to communicate
- Young people do not readily distinguish between 'online' and 'offline'
- Young people can and do form meaningful relationships online, with people they already know and people they meet online
- Young people often hold a lot of expert knowledge about new technologies and their uses but not all young people have the same levels of digital literacy
- Cyberbullying, sexting,[1] privacy breaches, identity theft and exposure to violent and sexually explicit content are potential risks for young people
- Strategies must reach beyond awareness raising and aim for long term behaviour change, developing resilience
- Strategies for young people need to address the digital literacy needs of both parents and the professionals who support them

Adults (18–64 years)

- Adults are prolific users of online platforms and services
- On average, those aged 25–64 years spend a minimum of 55% more time online via a computer than persons aged 18–24 years[2]
- Communication is a common online activity[3], and those aged 25–49 years account for 46–57% of social network users[4]
- Large numbers of adults report being exposed to cyber crimes such as online fraud, scams, and identity theft
- There is limited available research concerning the specific concerns and cyber safety risks encountered by this age group
- Developing adults' skills/knowledge will help minimise workplace cyber safety breaches, enhance productivity, promote consumer trust, and increase revenue from e-commerce



Seniors (65+ years)

- Older Australians are light users of the internet, less connected, and utilise the internet for different purposes than younger cohorts
- Email is the most common internet activity undertaken by Australian seniors, and is used primarily to stay in touch with friends and family[5]
- Seniors most commonly develop digital literacy via informal learning[6] and rely primarily on peers and family members for cyber safety information
- The key barriers to older Australians accessing the internet are lack of knowledge and skills, concerns about security and viruses and confusion about the technology[7]
- Seniors are the fastest growing age group in Australian society and sometimes have a significant asset base, making them ideal targets for cyber crimes
- Limited digital literacy remains the outstanding challenge for fostering seniors' cyber safety

Parents

- 46% of Australian parents feel they are well informed about cyber safety issues[8]
- Parents are most likely to use active mediation to foster their children's online safety, and want more information and resources to do so
- Many parents feel under-equipped to address the numerous and often complex safety issues their children might face online
- Most parents (91%) claim they are aware of their children's mobile phone and online usage, however teenagers overwhelmingly claim that this is not the case[9]
- Parents need to become more familiar with the platforms young people use and the attractions of using technology, as well as enhance their own technical skills
- To build parents' digital literacy further, it is important to foster intergenerational conversations about technology use.

DEFINITIONS

It is useful to define what is meant by 'cyber safety' and to highlight some of the key related concepts often used in discussions about how and why we might promote and support cyber safety

Cyber safety

'Cyber safety' – also referred to as 'online safety', 'internet safety', 'e-safety' or 'digital safety'– is broadly defined as "the safe and responsible use of Information and Communication Technologies (ICTs)".[10] Cyber safety addresses a wide range of issues including:

- online privacy (including the use of privacy settings);
- online etiquette (or 'netiquette');
- cyberbullying;
- sexting and 'sextortion' (extortion involving digital sexual imagery and distribution);
- online sexual predation and grooming;
- personal information security (e.g. keeping personal information such as images and identifying details safe);
- digital footprints (sometimes referred to as 'online reputation');
- safe social networking;
- accessing inappropriate content;
- internet and device addiction;
- safety when gaming online;
- security tools and filtering software;
- digital fraud;
- hacking;
- online piracy; and
- plagiarism.

Cyber safety strategies have conventionally focused on personal risks and protective measures. In recent years though, the emphasis has shifted towards more holistic solutions that recognise the importance of skilling populations not just to engage safely, but to ensure their online engagements maximise the potential of connectivity.[11] This shift demands that cyber safety strategies now embrace and promote digital inclusion, digital literacy, digital citizenship, and digital resilience.

Digital inclusion

Digital inclusion entails overcoming the 'digital divide' between the digital 'haves' and 'have nots'. Beyond the provision of access, digital inclusion initiatives seek to increase the scale and quality of opportunities for the broadest possible population to participate meaningfully in society using digital technologies,[12] enhancing learning, social capital, employment, and active participation in everyday civil society. Maximising digital inclusion requires the promotion of online safety for the broadest possible population.

Digital media literacy

Digital media literacy comprises the "technical and intellectual skills to access, understand, and participate in or create content on digital media and communications technologies".[13] There are three kinds of literacy required in a social media environment:

- technical literacy – being able to successfully navigate technologies with technical skills;
- media literacy – understanding the opportunities new technologies can open up; working knowledge of available platforms; capacity to make judgements about the quality and reliability of online sources; and
- social literacy – an understanding of the social norms that apply in online settings.[14]

Well developed digital media literacy enables users to make informed choices online.[15] Digital literacy influences users' ability to engage safely online because it guides decision making, interactions and interpretation of online information.

Digital literacy influences users' ability to engage safely online because it guides decision making, interactions and interpretation of online information

Digital citizenship

Digital citizenship describes the "skills, knowledge, and values required to be an effective, ethical and safe user of ICT".[16] There are five elements of digital citizenship:

- participation or 'civic engagement';
- literacies (digital, media, social);
- rights and responsibilities;
- norms of behaviour (appropriate and responsible online behaviour or 'good citizenship');
- sense of belonging (membership/ connection with others).[17]

Digital citizenship marks a shift to thinking about online practices as fundamentally social and community based practices, as opposed to purely individual ones.

Digital resilience

Digital resilience is the ability to deal with negative experiences online or offline.[18] Strategies focus on skilling users to adapt and respond effectively to potentially harmful online experiences.

Cyber safety has conventionally focused extensively on external/extrinsic protections (parental monitoring, rules, laws, parental control technologies, law enforcement, etc.). By contrast, digital resilience emphasises a more strengths based approach to cyber safety, which focuses attention on intrinsic/internal protections (e.g. self regulation, social literacy).[19]

The resilience perspective understands online engagements as just one dimension of everyday experience, recognising the potential for leveraging offline practices to support users' resilience online, and vice versa. Further, the resilience perspective reframes risk as potentially productive. For most population groups, "risk and resilience go hand in hand, as resilience can only develop through exposure to risks or stressful events."[20] However, for our nation's most vulnerable population groups, evidence suggests that whether or not risks translate into the experience of vulnerabilities depends on the support system surrounding an individual.[21]

01: TECHNOLOGY TRENDS AND CYBER SAFETY

Australians are among the earliest adopters of new technologies internationally, and are prolific users

The uptake of mobile technologies is perhaps the most significant technology trend currently impacting on cyber safety

Cyber safety initiatives must respond to constantly transforming technology trends, products and practices. Almost 90% of the Australian population uses the internet (as of June 2012), with 73% doing so more than once a day.[22] At the same time, Australians are embracing the shift to mobile technologies, transforming the ways they connect online. As audiences expand and new platforms appear, new online risks potentially emerge, and at times have attracted increased attention from media, policy makers and law enforcement agencies.[23]

While the rise of social media has occupied much media space and has tended to dominate recent developments in cyber safety, particularly in relation to young people, a range of other issues and trends also impact our capacity to respond effectively to the online safety challenge. These include the following.

Shift in the primary uses of online and networked media

Since the internet first emerged, the purposes for which users engage online have gradually transformed. Initially, users accessed the internet primarily for information seeking. Now, users engage primarily for communicative purposes. While popular perceptions suggest that young people are at the forefront of this trend, recent data shows that 25–49 year olds are also prolific users of social media.[24] Cyber safety and digital literacy initiatives need to be skilling users of all ages in the social norms of online engagement.

Cross-generational usage

Australians are among the earliest adopters of new technologies internationally, and are prolific users. There is strong cross-generational uptake, although uptake by Australian seniors continues to be more limited than other age groups.[25] Further, as the Australian population ages, the percentage of older Australians engaging with technologies regularly will steadily increase (e.g. users who currently engage with technology for work or leisure will not cease to engage online when they reach retirement age, although the purposes for which they go online may transform). With broad uptake now a real possibility, it is crucial that cyber safety strategies respond to the diverse demands of the age groups who are engaging online.

Maintaining credential privacy and credential based authentication remains a critical cyber safety issue. Young people, in particular, generally have limited awareness of such risks to their privacy

Rise of social media

In Australia, the use of social networking services increases every year with an 11% increase in the use of social networking sites in the period from 2009 (36%) to 2011 (47%).[26] Interestingly, those aged 25–49 years accounted for 46–57% of Australian users of social networking services.[27]

Social media are an integral part of the shift towards using ICTs for communicative purposes and are rapidly becoming integral to the conduct of business. For example, small businesses using social media to promote their services and products increased from 10% in 2010 to 27% in June 2012.[28]

Although social networking presents social and financial benefits, it also potentially exposes users to increased risks. Participation in social media sites such as Facebook entails the disclosure of personal information, which in turn comes with risks such as fraud, identity theft, and the sexual solicitation of children.[29] Further, the rise in cyberbullying has been attributed to the growth of social networking sites, particularly among children and young people.[30] Sharing of personal information and high volume usage reportedly increase these risks.[31] Malware is also a risk social networking users must navigate.

Rise of user-generated content and content-sharing platforms

New communicative and media practices are characterized by information connectedness, small scale digital content creation and peer-to-peer file sharing.[32] This shift means that 'consumers' become 'users' and creators – engaged in generating content to share with others. Attendant cyber safety challenges include disclosure of personal information, the protection of images and video, intellectual property, and the possibility of participating in illegal practices such as copyright theft and the exchange of inappropriate content. Users must be educated about the legal implications of their content production and sharing practices.

Uptake of mobile technologies

The uptake of mobile technologies – and in particular smartphones – is perhaps the most significant technology trend currently impacting on cyber safety. Factors of cost and portability are key drivers of the widespread uptake of mobile technologies. Connectivity, along with image and audiovisual capture capabilities, have transformed mobile phones from text and voice call technologies into full-blown pocket sized computers, with all the capabilities of a connected laptop.

The shift to mobile internet access entails a shift in the ways users experience connectivity. Whereas online interaction via a desktop computer can give users the feeling of entering a discrete 'online world', mobile access to the internet is folded into users' everyday real time and physical interactions, blurring the distinctions between 'online' and 'offline'.[33]

Cyber safety strategies must be capable of responding to the increasing prominence of mobile devices in everyday life, and in particular, the dominance of smartphones. The risks users encounter include privacy breaches (e.g. sexting[34]), identity theft, cyberbullying and exposure to malware. As of September 2012, there were up to "175,000 dangerous and high risk Android apps available for download through Google Play and third party app stores".[35] Further, when it comes to young people's technology use, mobility means that parents' traditional methods of moderating their children's online engagements are not as effective, highlighting the importance of digital literacy and regular conversations.

Cloud computing

Cloud computing is a form of internet based computing that enables people to store, access and share material such as photos, music, video content and emails; by using platforms such as Facebook, Wikipedia, Dropbox and YouTube to remotely access required material. Cloud computing has facilitated the growth in popularity of mobile technologies, as it enables devices to be synched remotely.

In the six months to May 2012, approximately 71% of the adult population in Australia used a cloud computing service.[36] Having generated $1.1 billion in revenue during the period of 2011–12, cloud computing remains both a popular access medium for the everyday user and a lucrative financial tool for Australian businesses.[37]

The ACMA notes that although the benefits of cloud computing are numerous, there are concerns regarding trust and privacy, service reliability, security and location of data storage.[38]

Platform integration

Platform integration, and in particular the use of single sign-on (SSO) mechanisms, allows users to access multiple service providers with a single credential.[39] Maintaining credential privacy and credential based authentication remains a critical cyber safety issue. Young people, in particular, generally have limited awareness of such risks to their privacy.[40]

The key barrier to Australian consumers participating in online commerce is diminished trust in the internet

GPS and location-based services

GPS enabled mobile devices and applications combine "real world data with virtual data"[41] to allow users to take advantage of services that use sophisticated location and positioning.[42] Devices that are GPS enabled include smartphones, tablets, and gaming consoles such as Xbox and Sony PSP.

Location based services have become particularly popular since the introduction of smartphones and tablets. Location based services are commonly accessed via mobile applications, including social media applications that identify friends' locations, turn-by-turn navigation, and listings of nearby cafes, restaurants and other amenities. Such services also allow users to locate their devices when they lose them. These services are expected to grow, with global revenue forecast to reach US$10.3 billion in 2015 (up from $2.8 billion in 2010).[43] In addition to the high uptake of smartphones, growth will be stimulated by mobile advertising, greater coverage and faster mobile network speeds, and the implementation of new business models.[44]

The ACMA notes that location based services – especially those that publish users' locations and other personal information – can potentially expose users to unwanted identification.[45]

Increase in e-commerce

There has been a significant increase in e-commerce in Australia over the last few years. In 2010 the ACMA found that 88% of respondents had performed an e-commerce activity in the previous six months. The ACMA also noted a substantial increase in the number of Australians undertaking shopping related activities online (7.81 million in June 2012; up from 6.16 million in June 2011).[46] Australians routinely use online banking and other forms of online financial management.

The key barrier to Australian consumers participating in online commerce is diminished trust in the internet.[47] In particular, consumers are concerned about information security and the trustworthiness of online retailers. Some also report uncertainty about how to use technology to make purchases. This underlines the importance of addressing cyber safety issues by promoting consumers' digital literacy.

Government services

Governments now rely heavily on their web presence to interface with the public. A number of local, state and federal government services have migrated or are migrating online to reduce pressure on face-to-face services (e.g. Centrelink). This benefits the consumer by reducing costs, increasing efficiency and providing digital services that can be accessed at any time.

However, information security, particularly as pertains to the potential vulnerabilities of large and/or inter-agency databases, remains a cyber safety issue. Further, the limited digital literacy of some users may also expose them to cyber safety risks.

Technologies in formal educational settings

Building on the popularity of new media technologies with young people, there has been significant investment globally in integrating technology into formal educational settings. A wide range of studies have begun to document the positive impacts of technology – especially laptops, mobile phones and tablets – on better engaging students in learning processes, enhancing learning outcomes, fostering school retention rates, and so on.

Nonetheless, uptake of technology in educational settings continues to be limited by:

- entrenched concerns about potentially exposing students to online risks while engaged in technology-facilitated learning;
- a lack of clarity about the lines of responsibility when educational institutions encourage technological engagement – which then spills over into extra-curricular time;
- blocking of social networking and other sites during school time; and
- banning the use of mobile technologies during school hours, etc.[48]

02: STRATEGIES TO ADDRESS CYBER SAFETY

Ultimately, the aim should be to shift all Australian users from thinking solely of cyber safety in terms that focus on risks and protections towards a framework of 'digital resilience' that encompasses critical digital and media literacy, continuous learning, social and emotional learning, and citizenship practices

Cyber safety needs to be considered against a transforming backdrop of technology trends, products and practices. Given that technology will continue to become ever more integrated into everyday life, it is important that cyber safety strategies are flexible and adaptable enough to respond to new opportunities and challenges as they emerge.

Who should we target?

Existing cyber safety strategies in Australia primarily target the practices of children and young people and, to a lesser extent, their parents. Although a continued focus on the cyber safety needs of these groups is important, there is an obvious need to direct information and resources to other groups that have been neglected by specific policies and programs to date.

There is a paucity of research data about adults' cyber safety practices and they are frequently overlooked within discussions of cyber safety yet represent the highest level of internet access among all ages.[49] While adults are active users of new communications technologies in Australian workplaces they are mostly *computer* literate but are not necessarily *internet* literate due to exposure to online technologies and applications relatively late in their careers. Adults represent a large consumer base for online products and services and therefore remain at high risk. Increasing adults' digital literacy and knowledge is key to minimising workplace cyber safety breaches, enhancing workplace productivity and building consumer trust and confidence.

Digital literacy remains a key issue for seniors and needs to be approached holistically. Initiatives need to foster seniors' technical skills but also their broader understanding of the benefits of connectivity. Strategies should promote an attitude of 'learning by discovery' and aim to produce users that can seek assistance, solve problems, and recover from any adverse online experiences. Given that young people frequently hold significant technological expertise, intergenerational cyber safety education strategies may provide an effective model for enhancing adults' and seniors' digital literacy; while also helping to promote increased understanding between generations about the use of technology.

There is also scope for cyber safety strategies to better respond to diversity within the key populations targeted by existing policy and programs. Research shows that those most at risk offline are correspondingly more at risk online, with marginalised young people identified in the USA and Australia as the group who are most vulnerable online. There is currently an untapped opportunity to address cyber safety knowledge and practice gaps affecting diverse groups within key populations.

In addition, small to medium sized enterprises (SMEs) is another group identified as at risk. Many struggle to stay abreast of technological change, often due to limited time or financial/human resources, and find it challenging to move out of 'self preservation' mode when it comes to managing online risks. This potentially inhibits their capacity to benefit from the digital economy. Strategies need to reward SMEs' participation with a time, financial or human resource benefit in order to be attractive to the target group.

From risk to resilience

Australian cyber safety strategies traditionally focused on the personal risks and necessary protective measures associated with the use of new media technologies. This focus was important in establishing cyber safety as a key issue affecting the Australian public and raising awareness within the community.

It is crucial that stakeholders in cyber safety foster a balanced public debate about the opportunities and risks of digital engagement

In recent years, however, there has been a shift within policy and practice towards more holistic and strengths based solutions that recognise the importance of skilling users not just to engage safely but to ensure their online engagements maximise the full potential of connectivity.

This means that principles of digital literacy, digital citizenship, digital inclusion and digital resilience increasingly underpin cyber safety strategies. Ultimately, the aim should be to shift all Australian users from thinking solely of cyber safety in terms that focus on risks and protections towards a framework of 'digital resilience' that encompasses critical digital and media literacy, continuous learning, social and emotional learning, and citizenship practices. By doing so, we are best positioned to enhance digital participation and safety for all Australians.

Importantly, in fostering a strengths-based approach, it is crucial that stakeholders in cyber safety foster a balanced public debate about the opportunities and risks of digital engagement, which enables users to make informed decisions about how they engage with new technologies. Cyber safety strategies should inform users about the potential risks of engaging online without overstating them, acknowledge the benefits of connectivity, and provide users with access to resources and tools to enhance their digital literacy.

Risks, harm and cyber safety

The relationship between risks, harm and online safety is complex. Emerging evidence overwhelmingly suggests that exposure to risk does not equate with harm and, indeed, some studies have shown that a certain degree of exposure to risk is necessary to the development of the kind of digital literacy that enables users to maximise their online safety. A user's awareness of risks does not necessarily result in long-term behaviour change and reduced online risk taking.

There are proven benefits to engaging online. To maximise the benefits of connectivity it is important for users to not only understand the risks of engaging online, but to also develop the necessary skills and strategies to deal with them effectively. Australia's response to cyber safety remains focused primarily upon campaigns and educational programs that seek to raise awareness about potential online risks. There is evidence to suggest that existing initiatives are successfully fostering a culture of community awareness around issues of cyber safety, but also that these strategies are now reaching saturation point.

New thinking in the field of cyber safety has begun to insist upon the prioritisation of strategies that broaden users' focus from awareness raising to long term behaviour change. While debates about the best mechanisms for achieving this are ongoing, there is clear evidence that experiential learning models – in which users are supported to navigate online risks and experience the consequences of their decision making processes – are more likely to enhance users' understanding of online safety issues and help them to develop the necessary skills, strategies and confidence to deal with them effectively.

User-centred programs, policies and products

Recent research indicates that cyber safety programs, policies and products are most effective when they are built upon processes of user engagement and participatory research and design.

User-centred approaches to cyber safety engage target audiences in:

- identifying, defining and prioritising online 'risks';
- generating the necessary research and practice based evidence about users' interactions; and
- drawing upon this knowledge to develop programs, policies and products that embed users' insights and experiences.

This ensures that cyber safety strategies connect into users' existing online and offline practices in a meaningful way, fostering maximum uptake and impact. Cyber safety initiatives should be regularly evaluated using the same processes to ensure their ongoing impact.

Online and offline

As more and more users embrace mobile technologies (e.g. smartphones and tablets), it is likely that the popular perception of a distinction between the 'online' and the 'offline' will recede. Research already shows that young people – the group of Australians that is most ensconced in the digital world – do not necessarily make this distinction, and that their decision making frameworks translate across online and offline domains. As a 2009 independent report noted, research showed that "some of the most troublesome risks are strongly associated with offline risks and that these two worlds do not exist independently. Thus, in order to address online risks, it is crucial that offline behaviours are also considered."[50] Wherever possible, cyber safety strategies should seek to leverage the relationship between online and offline to positive effect. Indeed, some have argued there is merit in approaching cyber safety as a part of a broader safety and wellbeing issue.

Users need to be encouraged to take on a 'continuous learning' attitude, whereby cyber safety and digital literacy are configured as key pillars of a lifelong learning approach

A long-term focus

Given the constantly evolving digital media landscape, short term approaches struggle to adequately prepare users to deal with continuously shifting online safety challenges and proliferating forms of technology. Users need to be encouraged to take on a 'continuous learning' attitude, whereby cyber safety and digital literacy are configured as key pillars of a lifelong learning approach to digital participation. This can only be achieved with forward thinking, long term strategies that endorse a shared digital responsibility, promote the digital resilience of Australians, and address the challenges of all groups in the community.

Increased coordination of the cyber safety agenda

A key issue for cyber safety policy making is to develop a comprehensive cyber safety policy framework that can address the specific needs of all groups of Australians.

To date, Australian responses to the challenge of cyber safety have been characterised by interventions that are frequently focused on:

- one or a few key issues (e.g. privacy, bullying, etiquette),
- a key population (e.g. children, seniors) and
- a setting (e.g. schools).

Evidence shows that the best way to promote cyber safety and digital citizenship is to create a culture change – across policy, industry, the community and individuals – that is supported by the ongoing development and provision of information, resources, programs and campaigns that are flexible enough to stay up-to-date with advances in the digital world. This involves moving from one-off interventions, resources and campaigns to looking at ways to join up learning and behaviour change opportunities.

Privacy, information security and the digital economy

A recent World Economic Forum (WEF) report projects that the current global decline in levels of consumer trust in the 'personal data ecosystem' will have a potentially significant impact on projected revenue from the digital economy.[51] Loss of trust can result from identity theft, security breaches and concerns over use of personal data by organisations. This highlights the need for industry and government to enhance privacy and information security mechanisms and rebuild users' trust regarding the use of personal and financial data and organisations' ability to protect personal information. Users should also have access to appropriate information on how to mitigate privacy and information security risks online.

Consumer trust

Trust in brand is crucial for industry. Cultivating trust not only mitigates the possibility of legal action but also encourages users to have positive experiences with digital services. The more confidence consumers have, the more time they are likely to spend online.

A 2012 World Economic Forum (WEF) report into use of personal data suggested the current decline in "trust of the personal data ecosystem" is having a significant impact on the financial revenue and projected revenue of organisations.[52] The report provided estimates of online retail growth; of particular interest is the influence of consumer perception on projected growth. If consumer trust is enhanced, it is projected that online retail will increase from US$2 trillion to US$2.5 trillion by 2016. However, should trust be eroded, this estimate declines to US$1.5 trillion.[53] This demonstrates the significant economic impact on online retail of restoring and enhancing consumer trust.

It is imperative that industry and government find ways to restore consumer confidence and trust in their ability to protect personal information; and provide appropriate information on how to mitigate risks online.

Targeted research and effective knowledge brokering

While Australian cyber safety efforts have been characterised by a high degree of cross sector and inter-organisational collaboration, the capacity for innovation and responsiveness is limited by both a funding environment that emphasises one-off commitments, and a lack of rigorous and current data pertaining to key populations. While longitudinal studies based on nationally representative samples provide important data about technology and cyber safety practices, equally, high quality qualitative research that is small scale, agile, iterative and participatory greatly enhances our capacity to understand the response requirements of new trends and practices.

It is imperative that organisations with an interest in enhancing cyber safety and digital participation focus attention on:

- the development of sustainable funding and investment models;
- the generation of research that is able to produce high quality data as new trends and practices emerge; and
- the development of effective knowledge brokering and translation.

03: CHILDREN (0–11 YEARS)

Children who take risks offline are more likely to engage in risky online behaviour

Technology use

A recent study of 26 nations showed that Australian children are among the youngest first time technology users in the world and that many access the internet on a daily basis.[54] Many parents use mobile devices to entertain their children when out and about.

Children use and access online technology in the following ways:

- Cartoon and television programs and associated websites;
- Handheld games consoles;
- Open and closed gaming websites;
- Role playing games[55] and online communities such as Club Penguin, where they can construct their own environment;
- Watching movies and listening to music;
- Moderated social networking platforms designed specifically for their age groups (e.g. Skooville, formerly SuperClubsPLUS);[56] and
- Despite age limitations, many children under the specified age have profiles and engage directly with social networking sites.

Some parents choose to purchase mobile phones for their children for safety reasons, for example, to ensure their children can contact them in an emergency.

Many children benefit from technology by learning and consolidating important skills such as reading, typing, and hand–eye coordination. Between the age of 10–11, children's networks begin to expand and they transition to using new technologies in ways that begin to make use of the full potential of connectivity.

Risks

Exposure to risk does not equate with harm. Indeed, emerging research indicates that some exposure to risk is necessary for children to develop digital literacy and resilience.[57] Further, not all children are at equal risk online. Children who take risks offline are more likely to engage in risky online behaviour.[58] Research has found that when asked, children themselves are also concerned about their own cyber safety[59] and understand risk as platform specific.

Cyber safety risks for children when using video sharing platforms, websites, social networking sites and games include but are not limited to:

- Exposure to pornography;
- Violent content;
- Contact and conduct risks;
- Cyberbullying and associated low self-esteem and emotional responses;[60]
- Contact with strangers and online predation;
- Content and practices that are not age appropriate through viewing media used by older siblings;
- Identity theft; and,
- Malware.

The potential for harm can be exacerbated by children's limited digital literacy skills.[61] One report noted, "children of [primary school] age are particularly challenged in their cognitive and emotional abilities to cope with online risk".[62] It follows then, that these risks increase where adult supervision is inadequate.[63]

MEASURES OF SUCCESS

Participation in educational internet safety interventions is associated with an increase in cyber safety awareness in children but not with a reduction of unsafe online behaviours.[69]

To be most effective, cyber safety education for children should:

- focus on exploration and frequency of use;[70]
- encourage ongoing experiential learning;[71]
- occur in spaces that children want to engage in;
- give children opportunities to explore and experiment with different strategies;
- allow children to make mistakes;
- facilitate immediate feedback;
- allow children to self correct;[72]
- establish clear ground rules;
- develop healthy consumption habits; and
- teach basic media literacy (e.g. the difference between fiction, fact and advertising).[73]

It is crucial that cyber safety strategies prepare children aged 7–8 for the higher risk transition years, when they begin to make full use of connectivity[74] and leverage sibling relationships to positive effect.

Over-monitoring can lead to children feeling distrusted and can undermine their ability to seek adult support when they encounter difficulties online

Responding effectively

Current initiatives supported by the Australian government, community and business organisations focus largely on educational campaigns and digital literacy initiatives that aim to foster cyber safety skills in children and are delivered in the school environment.

Examples of existing cyber safety initiatives include:

- The Alannah and Madeline Foundation's eSmart Schools Framework (centred on schools but founded on a whole of community approach to cyber safety);
- The ACMA's Cybersmart program (aimed at skilling parents, teachers, library staff, children and young people); and
- Skooville (a moderated online environment for primary school children).

A range of parental controls are available to ensure children's safe use of online devices. These range from 'soft' controls such as content filters or passwords to much more restrictive forms of control such as 'geo-fencing', whereby parents can undertake real time tracking of their children's devices and monitor their whereabouts. Many parents talk to their children about what they do online, stay nearby or sit with them when they use the internet, and encourage them to explore what they can do online.

Research indicates the following levels of parental engagement:

- 95% of Australian parents report that they actively mediate their child's safety online;[64]
- 72% of parents state they do what they can and "hope for the best";[65]
- 45% of parents claim they use filters or controls to block particular websites;[66]
- 48% of parents currently implement internet filters;[67] and
- 42% of parents use passwords and access controls.[68]

While a majority of parents do not feel that their child is at risk online, many parents claim they are "overwhelmed by the task of governing their child's behaviour online".

The importance of parental controls should not be overemphasised and some exposure to risk is necessary to developing digital resilience.

Over-monitoring can also lead to children feeling distrusted and can undermine their ability to seek adult support when they encounter difficulties online.

04: YOUNG PEOPLE (12–17 YEARS)

Young people draw upon the same moral framework that shapes their offline engagements

Technology use

Young people predominantly use the internet to socialise with friends, as a source of entertainment and amusement, and to communicate.[75]

Young people often engage online in the following ways:

- Social networking on sites and apps such as Kik, Instagram, Tumblr, YouTube and Twitter;
- Participate in 'remix' culture via digital creative content production;
- Online gaming, which is especially popular with young men;
- Listening, sharing and downloading music;
- Emailing and texting; and
- Searching for information to complete school work.

Technology use potentially offers young people a suite of important benefits[76] including the:

- Increase in media literacy;
- Support of formal and informal education;
- Exploration of creativity and identity;
- Sharing of creative outputs;
- Strengthening of interpersonal relationships;
- Sense of belonging and connection to their communities; and
- Formation of meaningful relationships online, with both people they already know and people met online.[77]

Young people do not readily distinguish between 'online' and 'offline', or online versus 'on phones', in the ways that adults do. Rather, they regard digital media as just another setting for their social interactions and often move seamlessly between various platforms and devices or navigate them simultaneously. This means that, rather than sliding into a moral vacuum when they go online, young people draw upon the same moral framework that shapes their offline engagements.[78] This underlines the importance of parents continuing to have open and ongoing conversations with young people about their online activities that reiterate their family's values. These conversations are an important backdrop against which young people make decisions online.[79]

To guarantee the greatest success and impact, cyber safety initiatives for young people must involve young people in conceptualising the issues, designing and implementing solutions

Awareness of the risks does not necessarily equate with reduced online risk taking by young people

Risks

Emerging research shows that young people today generally understand the range of risks they might face online, and most take active steps to protect themselves.[80] As with children, though, awareness of the risks does not necessarily equate with reduced online risk taking by young people.[81]

Risks faced by young people engaging in online activities include but are not limited to:

- Cyberbullying that can cause sleep loss, emotional distress and low self-esteem;
- Sexting;[82]
- Privacy breaches;
- Identity theft;
- Exposure to violent and sexually explicit content;
- The development of a negative digital reputation resulting from photos and the creation of an inappropriate yet permanent digital footprint; and
- Misunderstanding of the serious legal implications associated with illegally downloading music, or other breaches of copyright.

The risk of cyberbullying in this age group has been largely associated with social networking sites.[83] Research suggests a strong correlation between being bullied offline and being cyberbullied. Children aged 8–17 years are more than twice as likely to be bullied online if they have bullied someone else online.[84]

To guarantee the greatest success and impact, cyber safety initiatives for young people must involve young people in conceptualising the issues, designing and implementing solutions.

Strategies that engage young people in modelling cyber safety practices and mentoring their younger peers are most effective.

Cyber safety should move beyond the challenge of 'keeping young people safe' and find opportunities to use technology to enhance young people's wellbeing so that technology becomes part of the solution to complex social issues. For example, in some places in Australia, questions have been raised about the implication of social networking in teen cluster suicides.[91] It is now recognised that social media need to be included in suicide prevention strategies.

RESPONDING EFFECTIVELY

While young people's digital literacy and online practices are diverse, they often hold a lot of expert knowledge about new technologies and their uses. It is important that cyber safety education programs targeting young people do not overstate the risks of their online engagements.[85] Indeed, "recognising and acknowledging the positive impacts of online activity, may hold the key to overcoming issues of concern".[86]

To be most effective, cyber safety initiatives for young people should:

- Address perpetrators of bullying, as bullying others can be a sign of a young person in distress;
- Draw upon school-based cyber safety education, as well as the information and skills they gain through peer networks, sibling relationships and conversations with adults;
- Encourage the taking of calculated risks to develop digital literacy skills,[87] noting exposure to risk does not necessarily equate with harm;[88]
- Reflect on offline practices and peer relations to navigate potential risks;
- Reach beyond awareness raising and aim for long term behaviour change to develop resilience whether they are online or offline;
- Nurture digital literacy and emotional resources to "face, overcome and be strengthened by whatever it is they encounter online";[89]
- Alert them to the potential legal consequences of their online interactions (such as the Strong Choices cyber safety campaign featuring Tiwi Island band, B2M);
- Draw upon existing literature (for example, that developed by the National Children's Youth Law Centre) regarding legal rights and protections;
- Address the digital literacy needs of both parents and professionals who support young people (mental health workers, teachers, social workers, etc.);[90] and
- Leverage the connections between online and offline practices.

05: ADULTS (18–64 YEARS)

Adults aged 18–64 years are frequently overlooked within discussions of cyber safety yet more than two-thirds (67%) of those aged 18–34 years access the internet more than once a day, the highest level among all ages[92]

RESPONDING EFFECTIVELY

The most effective ways to address cyber safety for adults includes to:

1. Increase levels of digital literacy with particular reference to consumer trust;
2. Address the paucity of data for this age group's online behaviours;
3. Develop targeted campaigns, programs and products to visions of a digitally inclusive society;
4. Tackle this group's reservations about their online financial security[99] and concerns about online fraud and theft of personal information;
5. Examine sector specific digital literacy initiatives (e.g. psychologists are not always well-equipped to maximise the use of technology to support their work in clinical settings with young people with mental health issues).[100]

Developing this age group's technology and cyber safety skills and knowledge is key to minimising workplace cyber safety breaches, enhancing workplace productivity and building consumer trust and confidence.

Technology use

Some of the ways adults use technology include:

- Social networking, with those aged 25–49 years accounting for up to 57% of users;[93]
- E-commerce;
- Work or education based research; and
- Searching for general information.[94]

Of Australian adults who are regular online users:

- 82% frequently update their protective software;
- 61% use a firewall; and
- 50% use anti-spyware software.[95]

More than half (54%) of Australians over 18 years that go online regularly were "confident in their ability to manage security of personal information online".[96]

Risks

Adults are active users of new communications technologies in Australian workplaces. While they are mostly *computer* literate, a significant number may not be *internet* literate, and many have had to embrace the shift to Web2.0 and social media platforms late in their careers.

Large numbers of adults report exposure to cyber crimes such as:

- online fraud;
- general scams (adults aged 25¬–54 years reported the highest number of scams to ACCC);[97]
- identity theft; and
- online transaction scams.[98]

This age group constitutes a large consumer base for online products and services and is therefore at risk.

06: SENIORS (65+ YEARS)

Seniors are the fastest growing age group in Australian society and sometimes have a significant asset base, making them targets for cyber crimes

Technology use

Older Australians are light users of the internet, less connected, and utilise the internet for different purposes than younger cohorts. A 2011 report found that only 31% of those aged 65 years and over access the internet regularly.[101]

Seniors use technology to:

- Break down physical boundaries;
- Overcome social isolation; and
- Foster connections with family, friends, and those with whom they share common interests.[102]

Application-based online activities by seniors include:

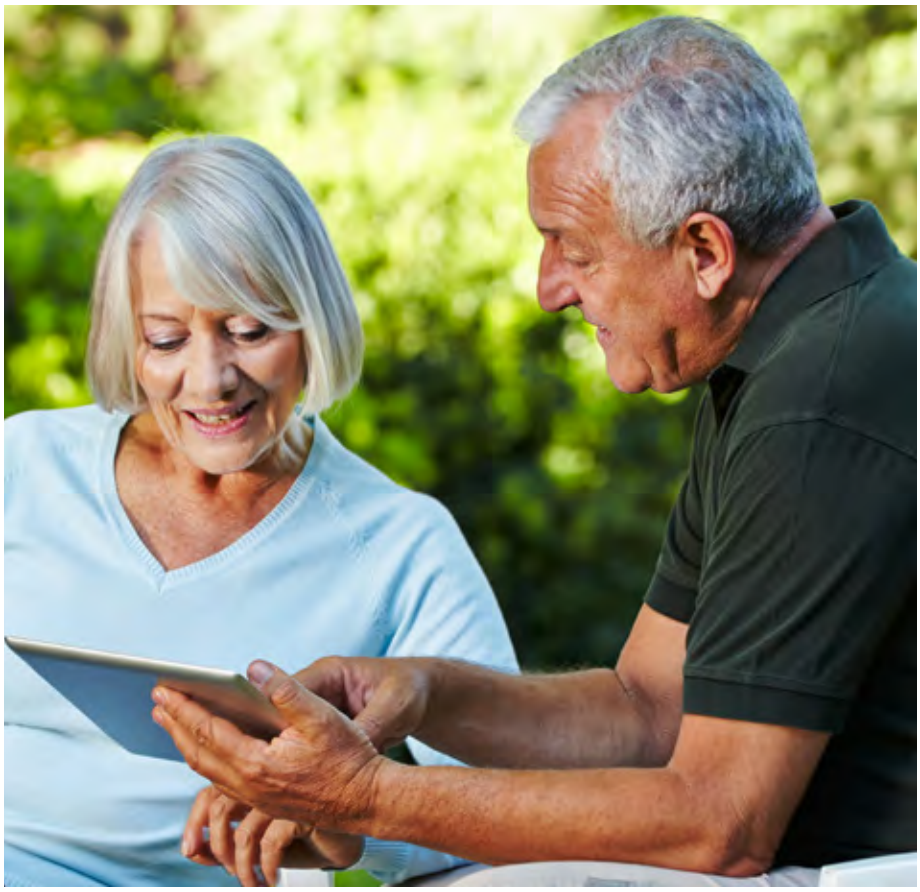
- Email to stay in touch with friends and family;[103]
- Skype to stay in touch with their children and grandchildren;
- Social networking services to connect with friends, family and events[104] (more than 500,000 Australian seniors aged over 60 currently have a Facebook page);[105]
- Paying bills, accessing news and current affairs stories and checking accounts;
- Searching for medical information.

Research indicates digital literacy rates for seniors are as follows:

- 78% report as 'self taught' through informal learning;[106]
- 54% report that they acquired computer skills 'at work';[107]
- 66% of those aged of over 65 stated they had 'very low' internet skills; and
- 50% stated that they had 'very low' computing skills.[108]

93% of seniors' online engagements happen at home with the following device use:

- 56% use a computer to access the internet;
- 23% use mobile phones; and
- 20% use tablets and smartphones to go online.[109]



Risks

The reported key barriers to older Australians accessing the internet are:

- lack of knowledge and skills (77%);
- concerns about security and viruses (64%); and
- confusion about the technology (74%).[110]

These factors also significantly impact on older Australians' capacity to practice effective cyber safety.

Risks faced by seniors online include:

- Identity theft;
- Personal information disclosure resulting in home burglaries;
- Inability to competently manage information security;
- Outdated virus protection software;
- Inadequate password protection or firewalls;[111] and
- Vulnerability to online scams, fraud and phishing.[112]

RESPONDING EFFECTIVELY

The most effective way to address cyber safety in seniors includes to:

- Help seniors understand the benefits of connectivity;[114]
- Increase seniors' levels of online engagement;[115]
- Address seniors highly divergent levels of understanding and skill;
- Generate awareness through conventional media such as radio, television and print media integrated with face-to-face delivery and hard copy resources.
- Target seniors in locations where they congregate (e.g. libraries, sporting and other clubs, nursing homes) to send the message that 'even if you're not connected, you may be affected'.

Research suggests that to minimise seniors' vulnerability to cybercrime, they either selectively use the internet or avoid it altogether,[113] indicating that finding ways to enhance seniors' competency and confidence is crucial to unlocking the benefits of connectivity for this cohort of users.

Given low levels of trust and familiarity with online modes of engagement, seniors are likely to prefer face-to-face and/or landline telephone based cyber safety services and education models.

Examples of existing successful initiatives include:

- The Tech Savvy Seniors collaborative initiative between the New South Wales Government, Telstra, and libraries and community colleges across New South Wales, which aims to provide low cost digital literacy education via participating libraries; and
- The Seniors Online Security Project – a Queensland based collaborative project with the Carindale PCYC, Queensland Police Service, the Office of the Information Commissioner and the Australian Government – that provides a combination of online and face-to-face cyber safety resources.

Evidence shows that seniors rely primarily on their peers and family members for information about cyber safety. Leveraging these relationships is thus an ideal way to spread the cyber safety message to older Australians. Intergenerational experiential education models – whereby young people work with seniors to guide them through scenario based learning exercises online – can enhance adults' digital literacy and their capacity to keep themselves safe online.[116]

07: PARENTS

Conversations provide opportunities for parents to reinforce the family values that shape and enhance their children's online experiences

Use of technical controls

Research shows that most parents are concerned about their children's online safety:

- 75% of parents minimise cyber safety risks by regularly installing and updating anti-virus software;
- 64% ensure that the computer is accessed in an open area that can be monitored;
- 48% use internet filters;
- 42% use passwords and access controls;[117] and
- 46% feel they are well informed about cyber safety issues.[118]

There is a clear need for accurate and up-to-date data around parents' cyber safety practices to inform future parental education initiatives.

Knowledge gap

Research indicated that parents are most likely to:

- Use active mediation to foster their children's online safety, and want more information and resources to do so;[119]
- Support their children's online safety centre primarily on overt or covert monitoring of their children's engagement with technology, and in particular their children's social networking activities;
- Have ongoing conversations with their children about online safety; and
- Know how to use online security tools and software.

Given mobile devices are increasingly the preferred point of access for children and young people, many parents feel under-equipped to address the numerous and often complex safety issues their children might face online.[120]

Generation gap

US research notes the generational gap between children's and parents' perceptions of cyber safety oversight:

- 39% of teenagers claim parents monitor closely;
- 84% of parents claim they monitor their teens' usage very/fairly closely; and
- 91% of parents claim they are aware of their children's mobile phone and online usage, teenagers overwhelmingly claim that this is not the case.[121]

RESPONDING EFFECTIVELY

To date, cyber safety education that prepares parents to support their children to manage online risks tends to be carried out through schools, and has conventionally consisted of seminars and workshops. A wide range of resources has been developed by government, industry and the not-for-profit sector to support the delivery of cyber safety education for parents. These resources generally encourage parents to communicate with their children about their online activities on a regular and ongoing basis; and aim to provide parents with a combination of technical and behavioural measures (e.g. use of privacy settings; setting limits) that can be used both to safeguard against children's potential exposure to risks and to promote healthy internet use.

The most effective way to address cyber safety for parents includes to:

- Build parents' familiarity with the platforms young people use and their technical skills;
- Understand the attractions of using technology; and
- Foster intergenerational conversations about technology use.

Many young people have skills and expertise in the use of technology, and this is potentially a significant resource for parents when enhancing their own digital literacy.

Conversations between generations can be of great benefit for parents. Sitting down with a young person in front of a computer, or with a tablet or mobile phone, and talking about how they use technology can help parents and children develop practical strategies to support their children's online safety.

Conversations provide opportunities for parents to reinforce the family values that shape and enhance their children's online experiences.[122] Making this a regular practice assists adults to gain the skills and confidence to have open and supportive conversations with their children about their technology use.

08: SUMMARY TABLES

The information contained in these tables summarises many of the data points presented in this report. The order of the data is not indicative of the relative importance, specific weighting or frequency of the individual risks, benefits or behaviours.

TABLE 1: KEY CYBER SAFETY RISKS BY POPULATION SEGMENT

Children	Young People	Adults	Seniors
Exposure to developmentally inappropriate content	Cyberbullying	Online fraud	Online fraud
Exposure to sexually explicit or violent content	Misuse of personal data	Online scams	Online scams
Cyberbullying	Sexting	Identity theft	Identity theft
Limited digital literacy skills	Sexual solicitation/predation	Limited or patchy use of internet security measures	Dating scams
Sexual solicitation/predation	Identity theft	Limited awareness of online safety resources	Limited digital literacy
Unsupervised use of the internet	Exposure to violent or sexually explicit content	Underestimation or lack of knowledge about risks	Limited or patchy use of internet security measures
Identity theft	Malware	Malware	Limited awareness of online safety resources
Malware	Piracy	Piracy	Underestimation or lack of knowledge about risks
			Malware

NB: The above table contains risks as they are currently identified in policy and practice.

TABLE 2: KEY BENEFITS OF ONLINE EXPERIENCE BY POPULATION SEGMENT

Children	Young People	Seniors
Hand–eye coordination	Media/Digital literacy	Connection to family, friends and communities
Reading and typing skills	Creativity and self-expression	Ease of banking and shopping
Educational benefits	Exploration of and experimentation with identity	Access to information
Creativity and self-expression	Sense of community, connection and belonging	Connection to local events
Media/Digital literacy	Strengthening personal relationships	General knowledge
	Civic engagement and political participation	Media/Digital literacy
	Wellbeing and resilience	
	Developing a sense of aspiration, personal achievement and self-worth	
	Educational benefits and general knowledge	

NB: Data not available for adults. At present the most rigorous evidence pertaining to the benefits of online engagement is provided by the research on young people.

TABLE 3: CYBER SAFETY STRATEGIES COMMONLY PRACTISED BY POPULATION SEGMENT

Children	Young People	Adults	Seniors
Don't share passwords	Ensure no one has access to personal or identifying information, through use of privacy settings	Regularly load updates to protective software	Regularly update internet security
Don't share personal information online (full name, street address etc)	Place limits on who they share their social networking posts with	Run frequent virus scans	Install security software
Inform parents when going online	Use strong passwords/ several passwords	Use anti-spyware	Install anti-virus software
Block people that don't observe internet etiquette	Don't share passwords	Change passwords frequently or use several passwords	Use several passwords
Tell parent/adult when something makes them feel uncomfortable online	Limit access to online profiles	Only surf trusted websites	Only shop online using secure web pages and payment
	Tell parent/adult when something makes them feel uncomfortable online	Don't share personal information with those outside their network	Use friends and family as reliable sources of information

NB: The above list is not exhaustive.

09: CONCLUSION

Initiatives aimed at improving the management of safety, security and privacy risks have undergone a gradual shift in emphasis. Whereas, previously, there was a sole focus on user protection, now the emphasis is on fostering trust and confidence in the online environment. Building an environment of trust and confidence necessitates a broader focus that forges user skills through mechanisms based on digital media literacy, as well as consumer protection arrangements.[123]

Ultimately, the aim should be to shift all Australian users from thinking solely of cyber safety in terms that focus on risks and protections, towards a framework of 'digital resilience' that encompasses critical digital and media literacy, continuous learning, behaviour change, and citizenship practices. By doing so, we will be best positioned to enhance digital participation and safety for all Australians.

ABOUT THE AUTHORS

Associate Professor Amanda Third

Principal Research Fellow,
Institute for Culture and Society,
University of Western Sydney

Associate Professor Amanda Third (PhD) is Principal Research Fellow in Digital Social and Cultural Research in the Institute for Culture and Society at the University of Western Sydney, and Research Program Leader in the Young and Well Cooperative Research Centre (CRC). Her research focuses on the socio-cultural dimensions of young people's technology use, with particular emphases on the intergenerational dynamics shaping technology practice, and vulnerable young people's technological engagements. She has an extensive track record in conducting large externally funded projects with industry organisations to examine young people's everyday technology practices. Since 2010, Assoc. Prof. Third has led Research Program 2: 'Connected and Creative', of the Young and Well CRC (youngandwellcrc.org.au). This research entity unites young people with researchers, practitioners, innovators and policy-makers from over 75 partner organisations across the not-for-profit, academic, government and corporate sectors to explore the role of technology in young people's lives, and how technology can be used to improve the mental health and wellbeing of young people aged 12 to 25. The research program Assoc. Prof. Third leads investigates how to better connect vulnerable young people with their communities by leveraging their technology practices and their creative engagements. She has been a member |of the Australian-based 'Technology and Wellbeing Roundtable' since 2008 and, in 2009, she was awarded the Murdoch University Medal for Early Career Research Achievement.

Pota Forrest-Lawrence

Research Assistant,
University of Western Sydney

Pota Forrest-Lawrence is a doctoral candidate at The University of Sydney Law School. Her PhD thesis interrogates the nexus between media and policy making by examining media representations of methamphetamine and its influence on illicit drug policies (legislation and regulations). She has worked on numerous research projects for government and non-government organisations as well as industry and the tertiary sector. Her research interests include drug law and policy, drugs, criminological theory, legal history, criminal law, policing and mental health, young people and risk, and crime prevention. She is the recipient of numerous scholarships including the Reca Stone Scholarship in Legal Theory, Ross Waite Parsons Award, The Cooke, Cooke, Coghlan, Godfrey and Littlejohn Scholarship and the John O'Brien Memorial Research Scholarship in Criminal Law and Criminology. She has taught subjects in criminology, social science, criminal justice and juvenile crime.

Anne Collier

Co-founder and Co-Director,
ConnectSafely.org

A journalist and youth advocate, Anne Collier is co-director of the nonprofit ConnectSafely.org and founder and executive director of Net Family News, Inc. She blogs at NetFamilyNews.org. Anne currently serves on the Aspen Institute Task Force for Learning & the Internet and in 2009-'10, she served as co-chair of the Obama administration's Online Safety & Technology Working Group, which delivered its report to Congress in June 2010, and prior to that on the Harvard Berkman Center's national Internet Safety Technical Task Force in 2008. With her co-director Larry Magid, she co-authored the first parents' guide to teen social networking: MySpace Unraveled (Peachpit Press, 2006) and several guidebooks helping parents navigate parenting in a digital age. She has spoken at numerous conferences throughout the US and internationally, contributed chapters to two books on youth and digital media, appeared on PBS Frontline's "Growing Up Online" (2008), been heard on public radio and nationally syndicated commercial radio in many states, and been quoted in the New York Times, Business Week, the Associated Press, and many other news outlets. Among other advisory roles, Anne currently serves on Facebook's Safety Advisory Board and helped the Born This Way Foundation form its Youth Advisory Board. She holds B.A. and M.A. degrees and lives with her family in San Jose, California.

REFERENCES

Australian Bureau of Statistics. "Australian Social Trends: Using Statistics to Paint a Picture of Australian Society". Canberra: Australian Bureau of Statistics, 2011.

———. "Internet Activity, Australia, June 2012: Mobile Handset Subscribers". Canberra: Australian Bureau of Statistics, 2012.

———. "Personal Fraud, 2010–2011". Canberra: Australian Bureau of Statistics, 2012.

Australian Communications and Media Authority (ACMA). "Australia in the Digital Economy: Consumer Engagement in E-Commerce". Melbourne, 2010.

———. "Click and Connect: Young Australians' Use of Online Social Media". Melbourne, 2009.

———. "Communications Report 2011–12, Series Report 3: Smartphones and Tablets Take-Up and Use in Australia". Melbourne, 2013.

———. "Developments in Internet Filtering Technologies and Other Measures for Promoting Online Safety. Second Annual Report to the Minister for Broadband, Communications and the Digital Economy". Melbourne, 2008.

———. "Digital Australians – Expectations About Media Content in a Converging Media Environment. Qualitative and Quantitative Research Report". Melbourne, 2011.

———. "Location services, personal information and identity". Melbourne 2012. http://www.acma.gov.au/theACMA/Library/researchacma/Research-reports/here-there-and-everywhere-consumer-behaviour-and-location-services

———. "Online Risk and Safety in the Digital Economy: Third Annual Report to the Minister for Broadband, Communications and the Digital Economy on Developments in Internet Filtering and Other Measures for Promoting Online Safety". Melbourne, 2009.

———. "Report 2: Australia's Progress in the Digital Economy – Participation, Trust and Confidence". Communications Report 2011–2012, Melbourne, 2012.

———. "The Government's Cybersafety Initiative". Melbourne, 2013. http://www.cybersmart.gov.au/About%20Cybersmart/What%20is%20Cybersmart/The%20Governments%20cybersafety%20initiative.aspx

———. "The Internet Service Market and Australians in the Online Environment". Melbourne, 2011.

———. "Use of Digital Media and Communications by Senior Australians". Melbourne, 2009.

———. "What Is Cybersmart?". Melbourne, 2013. http://www.cybersmart.gov.au/About%20Cybersmart/What%20is%20Cybersmart/Program%20principles.aspx

———. "What Is Digital Media Literacy and Why Is It Important?". Melbourne, 2009. http://www.acma.gov.au/WEB/STANDARD/pc=PC_311470; [site archived 30 May 2013]

Australian Competition and Consumer Commission. "Targeting Scams: Report of the ACCC on Scam Activity 2011". Canberra: ACCC, 2012.

Australian Government. "Australian Children's Cyber-Safety and E-Security Project: Report on the Results of a Parents' Survey". Wollongong: Department of Broadband Communications and the Digital Economy, 2010.

———. "Australia's Demographic Challenges: Appendix – The Economic Implications of an Ageing Population". Canberra: The Treasury, 2004. http://demographics.treasury.gov.au/content/_download/australias_demographic_challenges/html/adc-04.asp

———. "Cybersafety Help Button Download Page". Wollongong: Department of Broadband, Communications and the Digital Economy, 2013. http://www.dbcde.gov.au/online_safety_and_security/cybersafetyhelpbutton_download

———. "Digital Education Revolution – NSW – Digital Citizenship". Canberra: Commonwealth of Australia, 2010.

———. "Inquiry into Cyber Safety Issues Affecting Children and Young People: Submission to the Joint Select Committee on Cyber Safety". Sydney: Office of the Privacy Commissioner, 2010.

———. "Overview of Cybersafety Features of Social Networking Sites". Wollongong: Department of Broadband, Communications and the Digital Economy, 2012.

Australian Government Information Management Office. "Australians' Use and Satisfaction with E-Government Services". Canberra: Department of Finance and Deregulation, 2011.

Barr, Suzanne. *SuperClubsPLUS. Its Role in Cybersafety Education and Learning in Young Children.* Melbourne: SuperClubsPLUS, 2010.

bCyberwise. "bCyberwise Module Launched by the Prime Minister". McAfee Cybereducation, 2013. http://www.mcafeecybered.com/cybered/test/media.php

Blanchard, Michelle. *Navigating the Digital Disconnect: Understanding the Use of Information Communication Technologies by the Youth Health Workforce to Help Improve Young People's Mental Health and Wellbeing*. PhD thesis, Orygen Youth Health Research Centre: The University of Melbourne, 2011.

Blanchard, Michelle, Atari Metcalf and Jane Burns. *Bridging the Digital Divide: Young People's Perspectives on Taking Action*. Research Report No. 2, Inspire Foundation, October 2008.

Broadband for Seniors. "About". *Broadband for Seniors*, 2014. http://www.necseniors.net.au/about-bfs/

Bruns, Axel. Blogs, Wikipedia, Second Life, and Beyond. From Production to Produsage. New York: Peter Lang, 2008.

Byron, Tanya. "Safer Children in a Digital World: The Report of the Byron Review". Nottingham: Department for Children, Schools and Families, and the Department for Culture, Media and Sport, 2008.

Collier, Anne. "Digital Citizenship Reality Check: Notes from Nairobi's IGF". *NetFamilyNews*, 2011. http://www.netfamilynews.org/digital-citizenship-reality-check-notes-from-nairobis-igf

———. "Literacy for a Digital Age: Transliteracy or What?". *NetFamilyNews*, 2012. http://www.netfamilynews.org/literacy-for-a-digital-age-transliteracy-or-what

———. "Study on Long-Neglected Factor in Net Safety: Resilience". *NetFamilyNews*, 2013. http://www.netfamilynews.org/study-on-long-neglected-factor-in-net-safety-resilience

Collin, Philippa, Kitty Rahilly, Ingrid Richardson and Amanda Third. "The Benefits of Social Networking Services". Melbourne: Young and Well Cooperative Research Centre, 2011.

ConnectSafely. "Online Safety 3.0 – Empowering and Protecting Youth". Tech Parenting Group, 2012. http://www.connectsafely.org/online-safety-30-empowering-and-protecting-youth/

Couts, Andrew. "Facebook's 'Ask Our CPO' is just more privacy PR". Digital Trends. January 2013. http://www.digitaltrends.com/social-media/facebook-ask-our-cpo-privacy-pr/#!zhtFi

Cowling, David. "Social Media Statistics: Australia, January 2013". *SocialMediaNews*, 2013. http://www.socialmedianews.com.au/social-media-statistics-australia-january-2013/

D'Haenens, Leen, Sophie Vandoninck and Verónica Donoso. *How to Cope and Build Online Resilience?* EU Kids Online, 2013. http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20III/Reports/Copingonlineresilience.pdf

Digizen. "What Is Digital Citzenship?". Childnet International, 2013. http://www.digizen.org/digicentral/digital-citizenship.aspx

Dooley, Julian, Donna Cross, Lydia Hearn, and Robyn Treyvaud. *Review of Existing Australian and International Cyber-Safety Research*. Perth: Child Health Promotion Research Centre, Edith Cowan University, 2009.

Egan, Mark. "Digital Access and Literacy are Essential in Today's World". Infoxchange Australia, 2013. http://www.infoxchange.net.au/news/digital-access-and-literacy-are-essential-today's-world

Ewing, Scott, and Julian Thomas. "CCI Digital Futures 2010: The Internet in Australia". *Digital Futures*. Melbourne: ARC Centre of Excellence for Creative Industries and Innovation, Swinburne University of Technology, 2010.

Facebook. "Announcing the Launch of 'Ask Our CPO'". Facebook, January 2013. http://www.facebook.com/notes/facebook-and-privacy/announcing-the-launch-of-ask-our-cpo/501794623203758

———. "Safety in Numbers". Facebook, 2013. http://www.facebook.com/safety/community/

Family Online Safety Institute. *The Online Generation Gap: Contrasting Attitudes and Behaviors of Parents and Teens*. Washington: Family Online Safety Institute, 2012.

Google. "Good to Know: A Guide to Staying Safe and Secure Online". Google, 2013. http://www.google.com.au/goodtoknow/

———. "How You Can Protect Your Family Online".Google, 2013. http://www.google.com.au/intl/en/goodtoknow/familysafety/

Green, Leila, Danielle Brady, Kjartan Olafsson, John Hartley and Catharine Lumby. "Risks and Safety for Australian Children on the Internet: Full Findings from the AU Kids Online Survey of 9–16 Year Olds and Their Parents". Melbourne: ARC Centre for Creative Industries and Innovation 2011.https://www.ecu.edu.au/__data/assets/pdf_file/0009/294813/U-Kids-Online-Survey.pdf

Grubb, Ben. "Crimimals Breach Australian Tax System". *Sydney Morning Herald*,8 February 2013.

Hagen, Penny, Philippa Collin, Atari Metcalf, Mariesa Nicholas, Kitty Rahilly and Nathalie Swainston. Participatory Design of Evidence-Based Online Youth Mental Health Promotion, Intervention and Treatment. Melbourne: Young and Well Cooperative Research Centre, 2012. http://www.youngandwellcrc.org.au/document/ec72493f526cdb54a08990_a5ed5b0561/Young_and_Well_CRC_IM_PD_Guide.pdf

Howard, Jane. "Cybercitizens Must Be Resilient and Vigilant in a Digital World". Herald Sun,7 November 2012.

iiNet. "Online Safety". *iiNet Limited*, 2013. http://www.iinet.net.au/safety/

Infoxchange Australia. "Access Alone Is Not Enough". Infoxchange Australia, 2013. http://www.infoxchange.net.au/news/access-alone-not-enough

Internet Governance Forum. "Ei Workshop 122: Putting Your Trust in the Clouds: Why Trust Matters to the Open Internet". *Sixth Annual Meeting of the Internet Governance Forum*. Kenya: Internet Governance Forum, 2011.

———. "Ig4d 72: Good Practice Forum: Building Trust Environment for E-Commerce Challenges and Innovation". *Sixth Annual Meeting of the Internet Governance Forum*. Kenya: Internet Governance Forum, 2011.

Internet Safety Technical Task Force. *Enhancing Child Safety and Online Technologies*. Cambridge: Berkman Centre for Internet and Society, Harvard University, 2008.

Internet World Stats. "Australia, Internet Usage Stats and Telecommunications Market Report". *Internet World Stats*, 2012. http://www.internetworldstats.com/sp/au.htm

Ito, Mizuko, Kris Gutiérrez, Sonia Livingstone, Bill Penuel, Jean Rhodes, Katie Salen, Juliet Schor, Julian Sefton-Green and Craig S. Watkins. *Connected Learning: An Agenda for Research and Design*. Irvine: Connected Learning Research Network, 2013.

Jackson, Liz, and Mary Ann Jolley. "There Is No 3G in Heaven". *Four Corners*. Australian Broadcasting Corporation,10 September 2012.

Johnson, L, S Adams and M Cummins. *NMC Horizon Report: 2012 K–12 Edition*. Austin: The New Media Consortium, 2012.

Johnson, L, R Smith, A Levine and K Haywood. *The 2010 Horizon Report: Australia–New Zealand Edition*. Austin: The New Media Consortium, 2010.

Law Reform Committee. "Report of the Law Reform Committee for the Inquiry into Sexting". Melbourne: Parliament of Victoria, 2013.

Livingstone and Bulger, *Global Agenda for Children's Rights in the Digital Age.* Florence: UNICEF, 2013.

Livingstone, Sonia, Leslie Haddon, Anke Gorzig and Kjartan Olafsson. *Risks and Safety for Children on the Internet, The UK Report: Full Findings from the EU Kids Online Survey of UK 9–16 Year Olds and Their Parents*. London: London School of Economics, 2010.

Livingstone, Sonia, Lucyna Kirwil, Cristina Ponte and Elisabeth Staksrud, with the EU Kids Online Network. *In Their Own Words: What Bothers Children Online?* www.eukidsonline.net, 2013. http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20III/Reports/Intheirownwords020213.pdf

McAfee. *McAfee Digital Deception Study 2013, Exploring the Online Disconnect between Parents and Pre-Teens, Teens and Young Adults: US Research Topline Findings*. McAfee, 2013. http://www.mcafee.com/au/resources/reports/rp-digital-deception-survey.pdf

McGrath, Helen. *Young People and Technology: A Review of the Current Literature (2nd Edition)*. Melbourne: The Alannah and Madeline Foundation, 2009.

Meeker, Mary and Liang Wu. "Internet Trends @ Stanford – Bases". Kleiner Perkins Caufield Byers, 2012. http://www.kpcb.com/insights/2012-internet-trends-update

Microsoft. "Microsoft Computing Safety Index Shows Australia Is an Online Safety Leader". Microsoft, 2013. https://www.microsoft.com/australia/presspass/post/Microsoft-Computing-Safety-Index-shows-Australia-is-an-online-safety-leader

———. "Online Bullying Among Youth 8–17 Years Old: Australia". Microsoft, 2012.

Minato, Charlie. "Mobile Will Force Desktop into Its Twilight in 2014". *Business Insider Australia*, 2012. http://au.businessinsider.com/mobile-will-eclipse-desktop-by-2014-2012-6

Mishna Faye, Charlene Cook, Michael Saini, Meng-Jia Wu and Robert MacFadden. "Interventions for Children, Youth, and Parents to Prevent and Reduce Cyber Abuse". *Campbell Systematic Reviews*, 2009 (2). http://campbellcollaboration.org/lib/download/681/

Muir, Nancy C, and Linda Criddle. *Using the Internet Safely for Seniors for Dummies*. Hoboken: Wiley Publishing Inc, 2009.

National Research Council. *Youth, Pornography and the Internet*. Washington: The National Academies Press, 2002.

National Seniors Productive Ageing Centre. "Older Australians and the Internet: Bridging the Digital Divide". Melbourne: National Seniors Productive Ageing Centre, 2011.

Netsafe. "What Is Cybersafety?". *Netsafe*, 2013. http://www.cybersafety.org.nz/kit/welcome/cybersafety.html

Notley, Tanya. "Young People, Online Networks and Social Inclusion". *Journal of Computer-Mediated Communication*, 2009, 1208–27.

Office of the Victorian Privacy Commissioner. "Submission to the Victorian Parliament Law Reform Committee on Inquiry into Sexting". Melbourne: Office of the Victorian Privacy Commissioner, 2012.

Oliver, Kylie, Phillippa Collin, Jane Burns and Jonathan Nicholas. "Building Resilience in Young People through Meaningful Participation". *Advances in Mental Health*, 5(1) 2006: 34-40.

Optus. "Erasing Cyberbullying". *Singtel Optus Pty Limited*, 2013. http://www.optus.com.au/aboutoptus/About+Optus/Corporate+Responsibility/Cyber+Safety/Erasing+Cyberbullying

———. "Internet Safety: Internet Security – iCode Compliant". *Singtel Optus Pty Limited*, 2013. http://help.optuszoo.com.au/help/dial/safety/secure

Palmer, Sarah. "Where Do I Start? Female Seniors and the Internet". *Council on the Ageing (Western Australia)*, Sydney: Australian Communications Consumer Action Network, 2011.

Parliament of Australia. "Cybersafety for Seniors: A Worthwhile Journey – Second Interim Report: Joint Select Committee on Cyber-Safety". Canberra: Commonwealth of Australia, 2013.

———. "House of Representatives Committees – Inquiry into Cybersafety for Senior Australians". Canberra: Commonwealth of Australia, 2011. http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=jscc/senior_australians/index.htm

Pyramid Research. "Location-Based Services, Market Forecast 2011–2015 " Pyramid Research, 2011. http://www.pyramidresearch.com/store/Report-Location-Based-Services.htm?sc=PRN2062211_LBS

Queensland Police. "Senior Online Security". Queensland Police, 2012. http://www.police.qld.gov.au/programs/cscp/eCrime/sos.htm

Richardson, Ingrid, Amanda Third and Ian McColl. "Moblogging and Belonging: New Mobile Phone Practices and Young People's Sense of Social Inclusion". *DIMEA 2007: Second International Conference on Digital Interactive Media in Entertainment and Arts*. Perth: Murdoch University, 2007, 73–78.

Ross, Stuart, and Russell G Smith. "Risk Factors for Advance Fee Fraud Victimisation". *Trends and Issues in Crime and Criminal Justice*. Canberra: Australian Institute of Criminology, 2011.

Singh, Jazba, Michael Hartup, Michelle Blanchard and Jane Burns. "Cybersafety and Young People – Negotiating Responsible Digital Citizenship: Research Report". Melbourne: Young and Well Cooperative Research Centre, 2013.

Spielhofer, Thomas. "Children's Online Risks and Safety – A Review of the Available Evidence". London: UK Council for Child Internet Safety, 2010.

Telstra. "Telstra's Everyone Connected Program". Telstra, 2014. http://www.telstra.com.au/telstra-seniors/

The Alannah and Madeline Foundation. "eSmart Schools". The Alannah and Madeline Foundation, 2011. http://www.amf.org.au/eSmartschools/

ThinkUKnow. "Safer Internet Day 2014". ThinkUKnow, 2014. http://www.thinkuknow.org.au/site/sid14.asp

Third, Amanda and Ingrid Richardson. *Connecting, Supporting and Empowering Young People Living with Chronic Illness and Disability: The Livewire Online Community*. Centre for Everyday Life, Report prepared for the Starlight Children's Foundation, January 2010.

Third, Amanda, Ingrid Richardson, Philippa Collin, Kitty Rahilly and Natalie Bolzan. "Intergenerational Attitudes Towards Social Networking and Cybersafety: A Living Lab". Melbourne: Young and Well Cooperative Research Centre, 2011.

Third, Amanda, Damien Spry and Kathryn Locke. "Enhancing Parents' Knowledge and Practice of Online Safety: A Research Report on an Intergenerational 'Living Lab' Experiment". Melbourne: Young and Well Cooperative Research Centre, 2013.

Third, Amanda and Strider, Jess. "From Cybersafety to Digital Citizenship." Unpublished paper prepared for the Technology and Wellbeing Roundtable.

Trend Micro. "Android under Siege: Popularity Comes at a Price". *TrendLabs 3Q 2012 Security Roundup*, 2012.http://www.trendmicro.com.au/cloud-content/us/pdfs/security-intelligence/reports/rpt-3q-2012-security-roundup-android-under-siege-popularity-comes-at-a-price.pdf

Vodafone. "Cybersafety: Checklist for Young People". *Vodafone Blog*, 2012. http://community.vodafone.com.au/t5/Vodafone-Blog/Cybersafety-Checklist-for-young-people/ba-p/268804

———. "Resources for Parents". Vodafone Hutchison Australia Pty Limited, 2013. http://www.vodafone.com.au/aboutvodafone/corporateresponsibility/support-for-parents

Westcott, Sean, and Jean Riescher Westcott. *Digitally Daunted: The Consumer's Guide to Taking Control of the Technology in Your Life*. Herndon: Capital Books Inc, 2008.

World Economic Forum. "Rethinking Personal Data: Strengthening Trust". Davos-Klosters: World Economic Forum 2012. http://www3.weforum.org/docs/WEF_IT_RethinkingPersonalData_Report_2012.pdf

Young and Well Cooperative Research Centre. "Keep It Tame". Melbourne, 2013: Young and Well Cooperative Research Centre. http://keepittame.youngandwellcrc.org.au/

Yu, Jiangshan, Guilian Wang and Yi Mu. "Provably Secure Single Sign-On Scheme in Distributed Systems and Networks". IEEE Computer Society, 2012.

Zajac, Ian T, Ingrid HK Flight, Carlene Wilson, Deborah Turnbull, Steve Cole and Graeme Young. "Internet Usage and Openness to Internet-Delivered Health Information among Australian Adults Aged over 50 Years". *Australasian Medical Journal*, 5 (2012): 262–67.

ACKNOWLEDGEMENTS

The authors wish to thank Dr Philippa Collin for her feedback on this report, and Bettina Rösler and Kari Pihl for their contribution to this publication.

The authors also wish to thank Nancie-Lee Robinson and Shelly Gorr, of Telstra's Chief Sustainability Office, for their contribution to the report.

University of Western Sydney

The University of Western Sydney (UWS) is a modern research-led metropolitan university that was established in the late 1980s. UWS nurtures a distinctive, high-impact research culture, committed to enhancing our region's cultural, economic, environmental and educational development, and is responsive to contemporary challenges in Greater Western Sydney and beyond.

uws.edu.au

ENDNOTES

1 It should be noted that recent research suggests that sexting should not be regarded primarily as an online risk. While sexting deploys digital media, it is a social and health issue that is most effectively addressed through education and programs targeting sexual health, sexual harassment/exploitation and/or dating violence.

2 ACMA, "Report 2: Australia's Progress in the Digital Economy", 11.

3 Ibid, 14.

4 Ibid., 22.

5 Palmer, "Where Do I Start? Female Seniors and the Internet", 5; ACMA, "Report 2: Australia's Progress in the Digital Economy", 14.

6 ACMA, "Use of Digital Media and Communication by Older Australians".

7 National Seniors Productive Ageing Centre, "Older Australians and the Internet", 9–10.

8 Australian Government, "Australian Children's Cyber-Safety and E-Security Project", 33.

9 Family Online Safety Institute, *The Online Generation Gap*, 2.

10 Netsafe, "What is Cybersafety?".

11 A Young and Well Co-operative Research Centre project focusing on young people's online practices found that "there are a number of significant benefits associated with the use of [social networking services (SNS)] including: delivering educational outcomes; facilitating supportive relationships; identity formation; and, promoting a sense of belonging and self-esteem. Furthermore, the strong sense of community and belonging fostered by SNS has the potential to promote resilience, which helps young people to successfully adapt to change and stressful events. Importantly, the benefits of SNS use are dependent on good internet and media literacy: having the skills to critically understand, analyse and create media content. Maximising the benefits of SNS and promoting internet and media literacy may help protect young people from many of the risks of online interaction, such as cyber-bullying, privacy breaches and predation. For example, understanding how to produce creative content and manage the distribution of this content supports fully informed decision making and assessment of one's own, and others', privacy" (Collin et al. "The Benefits of Social Networking Services", 7).

12 Notley, "Young People, Online Networks and Social Inclusion".

13 ACMA, "Developments in Internet Filtering Technologies and Other Measures for Promoting Online Safety", 51.

14 Collier, "Literacy for a Digital Age." Henry Jenkins identifies 11 categories of digital literacy. See http://www.newmedialiteracies.org

15 ACMA, "What Is Digital Media Literacy and Why Is It Important?".

16 Netsafe, "What Is Cybersafety?". ACMA's definition comprises three elements: digital etiquette, digital literacy and digital security. Refer to ACMA, "Developments in Internet Filtering Technologies and Other Measures for Promoting Online Safety", 51, for a more detailed explanation of the concepts digital etiquette, digital literacy and digital security.

17 Collier, "Digital Citizenship Reality Check".

18 D'Haenens et al., "How to Cope and Build Online Resilience?", 2.

19 D'Haenens et al.'s pioneering work on (digital) resilience distinguishes three categories of online and offline coping strategies: a) fatalistic/passive or passive coping (hoping the problem will go away by itself, not using the internet for a while); b) communicative coping (talking to somebody about the problem); c) proactive coping or problem solving (trying to fix the problem, deleting unwelcome messages online, blocking a sender online) (Ibid., 2).See also Collier, "Study on Long-Neglected Factor in Net Safety: Resilience".

20 D'Haenens et al., "How to Cope and Build Online Resilience?", 2.

21 Livingstone and Bulger, *Global Agenda for Children's Rights in the Digital Age* (UNICEF, 2013: 16).

22 ACMA, "Report 2: Australia's Progress in the Digital Economy", 9; Internet World Stats, "Australia, Internet Usage Stats and Telecommunications Market Report".

23 Livingstone et al., "Risks and Safety for Children on the Internet", 13.

24 ACMA, "Report 2: Australia's Progress in the Digital Economy", 21.

25 ACMA, "Use of Digital Media and Communications by Senior Australians", 1–2.

26 Australian Government Information Management Office, "Australians' Use and Satisfaction with E-Government Services", 8.

27 ACMA, "Report 2: Australia's Progress in the Digital Economy", 22.

28 Ibid.

29 ACMA, "Online Risk and Safety in the Digital Economy", 2.

30 ACMA, "Click and Connect", 35.

31 ACMA, "Online Risk and Safety in the Digital Economy", 18.

32 Richardson et al., "Moblogging and Belonging".

33 Ibid.

34 One of the most highly publicised cases of sexting in Australia is that of DPP v Eades [2009] NSWSC 1352. It was the first case in New South Wales that involved the prosecution of the act of sexting. Eades was charged with inciting a person under 16 to commit an act of indecency and possession of child pornography under the *New South Wales Crimes Act 1900*. Sexting can give rise to negative effects such as anxiety, mental anguish, depression and suicide (Office of the Victorian Privacy Commissioner, "Submission to the Victorian Parliament Law Reform Committee Inquiry into Sexting", 7).

35 Trend Micro, "Android under Siege", 2.

36 ACMA, "Report 2: Australia's Progress in the Digital Economy", 17.

37 Ibid., 18.

38 Ibid.

39 Yu et al., "Provably Secure Single Sign-On Scheme in Distributed Systems and Networks".

40 Australian Government, "Inquiry into Cyber Safety Issues Affecting Children and Young People", 6.

41 Johnson et al., "The 2010 Horizon Report", 15.

42 Johnson et al., "NMC Horizon Report", 12.

43 Pyramid Research, "Location-Based Services".

44 Ibid.

45 ACMA, "Location Services", 123.

46 ACMA, "Report 2: Australia's Progress in the Digital Economy", 2.

47 ACMA, "Australia in the Digital Economy", 22.

48 Ito et al., "Connected Learning".

49 ACMA, "The Internet Service Market and Australians in the Online Environment", 31.

50 Dooley et al., *Review of Existing Australian and International Cyber-safety Research*, 13.

51 World Economic Forum, "Rethinking Personal Data: Strengthening Trust", 5.

52 Ibid., 5.

53 Ibid., 9.

54 Green et al., "Risks and Safety for Australian Children on the Internet", 7.

55 ACMA, "Click and Connect".

56 Barr, *SuperClubsPLUS*.

57 D'Haenens et al., "How to Cope and Build Online Resilience", 2. See also Collier, "Study on Long-Neglected Factor in Net Safety: Resilience."

58 Barr, *SuperClubsPLUS*, 6.

59 Ibid.

60 Ibid.

61 Green et al., "Risks and Safety for Australian Children on the Internet", 17; Barr, *SuperClubsPLUS*, 6.

62 Ibid.

63 ACMA, "Online Risk and Safety in the Digital Economy", 3.

64 Green et al., "Risks and Safety for Australian Children on the Internet", 42.

65 McAfee, *McAfee Digital Deception Study 2013*, 16.

66 Green et al., "Risks and Safety for Australian Children on the Internet", 47.

67 Australian Government, "Australian Children's Cyber-Safety and E-Security Project", 33.

68 Ibid.

69 Barr, SuperClubsPLUS, 11.

70 Ibid.

71 Ibid.

72 Ibid.

73 Green et al., "Risks and Safety for Australian Children on the Internet", 10.

74 Barr, SuperClubsPLUS, 6.

75 ACMA, "Report 2: Australia's Progress in the Digital Economy", 14.

76 Collin et al., "The Benefits of Social Networking Services".

77 Third and Richardson, *Connecting, Supporting and Empowering Young People Living with Chronic Illness and Disability*.

78 Third et al., "Intergenerational Attitudes Towards Social Networking and Cybersafety".

79 Ibid.

80 Third et al., *Enhancing Parents' Knowledge and Practice of Online Safety*.

81 Mishna et al., "Interventions for Children, Youth, and Parents".

82 It should be noted that recent research suggests that sexting should not be regarded primarily as an online risk. While sexting deploys digital media, it is a social and health issue that is most effectively addressed through education and programs targeting sexual health, sexual harassment/exploitation and/or dating violence.

83 ACMA, "Click and Connect", 35.

84 Microsoft, "Online Bullying Among Youth 8–17 Years Old", 1.

85 McGrath, Young People and Technology.

86 Singh et al., "Cybersafety and Young People "Negotiating Responsible Digital Citizenship: Research Report", 8.

87 Green et al., "Risks and Safety for Australian Children on the Internet".

88 Collier, "Study on Long-Neglected Factor in Net Safety: Resilience".

89 Michael Carr-Gregg, cited in Howard, "Cybercitizens Must Be Resilient and Vigilant in a Digital World".

90 Blanchard, *Navigating the Digital Disconnect*.

91 Jackson and Jolley, *There Is No 3G in Heaven*.

92 ACMA, "The Internet Service Market and Australians in the Online Environment", 31.

93 Ibid., 22.

94 ACMA, "Online Risk and Safety in the Digital Economy".

95 ACMA, "Report 2: Australia's Progress in the Digital Economy", 26.

96 ACMA, "Digital Australians", 67.

97 ACCC, "Targeting Scams", 4.

98 Ross and Smith, "Risk Factors for Advance Fee Fraud Victimisation", 4.

99 ACMA, "Use of Digital Media and Communications by Senior Australians", 8.

100 Blanchard, *Navigating the Digital Disconnect*.

101 ABS, "Australian Social Trends", 26.

102 Ewing and Thomas, "CCI Digital Futures 2010", 12.

103 Palmer, "Where Do I Start? Female Seniors and the Internet", 5; ACMA, "Report 2: Australia's Progress in the Digital Economy", 14.

104 Parliament of Australia, "Cybersafety for Seniors", 11.

105 Ibid, 15.

106 ACMA, "Use of Digital Media and Communication by Older Australians".

107 Parliament of Australia, "Cybersafety for Seniors", 158.

108 National Seniors Productive Ageing Centre, "Older Australians and the Internet", 18. Some seniors may be placing themselves at risk because they conflate computer literacy with web literacy. A government website claims that "those who used a computer during their working lives are sometimes at risk because they believe that, because they can use a computer, they know how to use the internet" (http://www.atg.wa.gov/internetSafety/seniors.aspx#.USQdDo7YZ8w).

109 Parliament of Australia, "Cybersafety for Seniors", 156.

110 National Seniors Productive Ageing Centre, "Older Australians and the Internet", 9–10.

111 Ibid, 23.

112 Ibid, 26.

113 Ibid, 45.

114 Ibid, 24.

115 ABS, "Australian Social Trends", 26.

116 Third et al., "Intergenerational Attitudes Towards Social Networking and Cybersafety".

117 Australian Government, "Australian Children's Cyber-Safety and E-Security Project", 33.

118 Ibid, 2.

119 Green et al., "Risks and Safety for Australian Children on the Internet", 11.

120 Third et al., "Enhancing Parents' Knowledge and Practice of Online Safety".

121 Family Online Safety Institute, *The Online Generation Gap, 2*.

122 Third et al., "Enhancing Parents' Knowledge and Practice of Online Safety."

123 ACMA, "Online Risk and Safety in the Digital Economy".

IT'S HOW
WE CONNECT

telstra.com.au/cyber-safety

JULY 2014