Life Activities Clubs Victoria Inc
Registered Incorporated Association: A0054351A ABN: 85 104 164 408

Joint Select Committee on Cyber-Safety

Inquiry into Cybersafety for Senior Australians

Submission by Life Activities Clubs Victoria Inc.

Who we are
Life Activities Clubs Victoria Inc. (LACVI) represents a network of incorporated Life Activities Clubs throughout Victoria that are run by volunteers on a non-profit basis.

Life Activity Clubs provide people in retirement or approaching retirement (typically aged 50 and over) with opportunities to enjoy a full, satisfying and connected community life and maintain lifelong wellbeing.

There are currently 22 Life Activities Clubs in Victoria (including 5 in regional centres) with each Club offering its members a wide range of recreational and social activities that provide physical, mental and social stimulation. The activities provided for the 4000 club members are determined by the interests of the members of each club.

Submission

It is obvious that views differ widely across our membership and it is therefore not possible for any submission adequately to represent the breadth of opinion from such a diverse constituency. Having said that, the primary author of this submission is himself a senior, immersed in a range of seniors' organisations and having considerable experience analysing and interpreting his cohort's needs and aspirations.

He has been involved in the IT industry since 1964 and was a pioneer and key thought leader in e-business systems, infrastructure and developments across Australia from 1992 to 2000 when he commenced his own e-business consultancy practice. He was a volunteer member of CPA Australia's Information Management and Technology Centre of Excellence for over 12 years and although now semi-retired, he is still involved in the e-world and manages a Broadband for Seniors kiosk on behalf of his local U3A.

Against this background, the following comments are provided on the issues relevant to this Inquiry.

Précis
To outline our overall thesis, the following issues appear to be most important:

- Although some seniors may be more vulnerable than others, cybersafety is not specifically a seniors' issue.
- Seniors, particularly Fourth Age seniors, are likely to benefit very significantly from increased use of modern communication technologies.

- There is a need for a strong, ubiquitous educational campaign, particularly using traditional media, to explain the benefits of the Internet and encourage people to use the available technologies.
- By its nature, such a campaign must preclude scaremongering.
- The educational campaign must also emphasise the simplicity (and safety) of using these technologies and provide information on where basic skills can be acquired, either free or at very low cost. (Quite a few opportunities already exist, but are poorly promoted and consequently under-utilised.)
- Basic protection mechanisms should be mandated for all Internet-enabled devices. This should include automatic updating antivirus, antispam, phishing, spyware, etc., protection and a firewall, intrusion and identity protection – and whatever else becomes necessary as fraudsters keep pace with technological advances.
- Seniors should have the cost of such protection subsidised to ensure it is maintained and updated as required.
- A secondary educational campaign (similar in nature to that described above) should to instituted to encourage users to protect themselves against their own stupidity, including risk-taking behaviour. This should include references to the common risks (Nigerian Bankers, Billion Dollar Lottery wins, Business or Employment offers that are too good to be true, etc.), but major on defence mechanisms (don't do things in cyberspace that you wouldn't do in the real world, if it looks too good to be true….., and so on).

Defining the Issues

There appears to be a premise inherent in the basis of this Inquiry that senior Australians are in some way different from other Australians. This premise is open to challenge and unless senior Australians are defined to mean only people older than, say 80 or 85, it may well be invalid. Even then, there are quite a few octogenarians and nonagenarians with cyber-skills that would shame many people 50 years younger.

Seniors are usually defined as those exceeding 50 years of age, or perhaps 55 for the purposes of some superannuation regulations, or 60 for eligibility for a Seniors Card or a little more for the Age Pension, but a large proportion of all of those groups used computers, including many web-based applications, during their working lives (and many still work and/or still use computers all day, every day). Given this, it is suggested that for the most part, there is little to differentiate the cybersafety needs of 'seniors' for those of the rest of the community.

Granted, there is a section of the older population who are not comfortable with new technology (of any sort), but they probably protect themselves fairly effectively by simply declining to use the technology at all. This is very unfortunate because a strong case can be made that use of up-to-date communication technologies can, and often does (certainly should), be a key mechanism for the very old or infirm in maintaining connectivity and engagement with family and friends. In some cases, it may also be their only means of conducting their necessary day-to-day business – banking, paying bills, online purchasing and so on.

For this sector of the community (and fear of the technology is by no means limited to any age-group other than the very young), there is a compelling argument to educate people, to demystify and simplify the processes, to encourage universal adoption of, at least easy familiarity with, electronic technologies. There is a clear role for government in this regard, but not one it has either been acknowledged or implemented at all well.

Equally, there are many ‘non-seniors’, younger people, typically tradespeople, manual workers, home-makers and so on, who are not routinely exposed to computers and communication technologies who are at risk when they first start to explore the cyber-world. Although the messages may be targeted a little differently, these people need essentially the same assistance and safety mechanisms that appear to be the objective of this Inquiry.

It is our contention that the disproportional emphasis on risk, particularly risk that is (strangely) attributed to the Internet, is counterproductive to people benefitting from the technologies available across the community today. ALL people should be strongly encouraged to avail themselves of the benefits of modern technologies and simply be given a few gentle reminders that they should not expose themselves to risks on the web that they wouldn’t happily accept in the real world.

Although this message may be relevant to many people in the community, it has particular relevance to people who do not access the Internet routinely. It therefore needs to be disseminated via traditional media at least as ubiquitously as by electronic media.

Government has a responsibility to educate all people about the benefits of using information technologies extensively – and this education should balance the benefits against the risks, without unduly emphasising risk. This is particularly important given the shift to providing almost all information via both government and commercial websites.

There are some basic protections that should be provided on every device capable of accessing the Internet. Any of the popular Internet security software packages available would appear to provide quite strong protection against cyber-attacks. Software that is self-updating and that provides a fire-wall/intrusion protection, anti-virus and spyware software, anti-phishing and identity protection, and possibly a spam filter probably comprise the basic package and should be mandatory on all Internet enabled devices. Beyond that, most of the safety package is pre-installed (or not) in the human brain.

Given that many older people are on fixed incomes, many of them quite low, **government could subsidise the cost of proper security protection for seniors, perhaps on a $ for $ basis, but all Internet enabled devices should be pre-installed with suitable cybersafety software.**

The greatest danger arising from use of the Internet is the extent of criminal activity by unscrupulous individuals preying on the greed and gullibility of the users.

The oft-repeated message about the risks of sending one’s credit card details over the Internet has been highly effective, even though it is largely misinformed and misdirected. Criminals with the resources to invest in devices that lay in wait for the nano-second or two during which an individual’s credit card number is transmitted from one point to another are far more likely to direct their investment into purchasing a million valid numbers from another unscrupulous business, or in simply breaching the security of an organisation storing customer data, including credit card data, for long periods, allowing the criminals to access this data at their leisure, rather than while it is in transit. Numerous other examples can be given to demonstrate that the ‘popular’ risks of the internet are often more perceived than real.

This is not to say that there are no risks – simply that the conventional wisdom is often quite misguided and remedies are therefore poorly targeted.

Ideally, government should focus its efforts on making Internet crime unprofitable, but it is unlikely that any government would or could marshal sufficient resources to do this effectively. Certainly, transnational intelligence and enforcement action should continue, preferably on a much greater scale, but educating all Australian users about the common risks (phishing, scams, etc.) and how to combat them would be a relatively easy short-term task. By encouraging individuals to ensure that cyber-criminal attacks against them are unproductive and therefore uneconomical would be a significant step forward.

It is hard to imagine that people are still being duped by such common web-based practices as phishing, variations on Nigerian Banker scam, the billion dollar lottery wins, even very unsophisticated virus attacks (and their complementary hoaxes) and so on. All of these devices and subterfuges have been widely publicised and it is almost inconceivable that people continue to fall victim to their own greed and gullibility.

Government should endeavour to combat this with a ubiquitous advertising campaign highlighting the typical guises in which these scams arrive and advising people that if it smells like rotten fish, it may well be rotten fish. Similarly, if it looks too good to be true, it more assuredly is.

It is difficult to identify issues that are especially relevant to seniors' safe use of the Internet, but cost is probably a major one. Many seniors are likely to try to do it 'on the cheap' to avoid spending any more than necessary of their often meagre income. It is for this reason that we suggest government should subsidise the cost of security software/devices and perhaps access to broadband services and even other access devices and software. **Certainly, training should be freely available to ensure older people are able to use the Internet extensively and safely. There are already some services providing assistance, e.g., the Broadband for Seniors program, but they are limited in scope and do not currently teach anything about cyber-safety or social media, business use of the Internet or many other skills our tutors are regularly asked about.** There is a clear need for this and government has a role to ensure seniors are not excluded from their use simply because they cannot afford high-cost and poorly targeted services that might provide some of these skills.

Providing a safe environment, no matter how superficial, would encourage seniors to make greater use of the internet – and to do so with minimal risk.

Specific Responses to Terms of Reference

a) The extent of risk experienced by many seniors is not noticeably different from that across the whole community although some (mainly older) seniors may be more trusting or gullible (or simply uninformed) than others.

b) Too many seniors respond to the scaremongering and ill-informed comments about risk by simply not using the technology. This is a serious community issue, increasing the cost of many services through duplicated communication channels, but more importantly, excluding many older or infirm seniors from important business and personal support mechanisms.

c) There is a compelling need for government to provide at least two education programs free of charge to all seniors. The first should encourage the greatest possible use of the Internet by seniors, focussing on the benefits rather than the risks. The second should identify (but not overstate) the common risks and explain how to avoid them or deal with them safely. A third educational program to teach a range of basic skills should also be considered – things such as social media, Internet banking, basic word processing, perhaps even some simple graphics, and so on, on a heavily subsidised basis. This should include safe behaviours and risk assessment skills.

d) There is little any single government (or even group of governments) can do to reduce the extent of cybercrime without very strong universal laws and a huge international investment in investigations and enforcement. This will never happen so the best we can hope for is much stronger policing within Australia. This should be combined with an advertising campaign designed to make criminal activity on the Internet less effective and much less profitable.

Lindsay Doig
President
20 January 2011