Addressing the cybersafety challenge: from risk to resilience

August 5, 2014

by rcrellin

This report, comissioned by Telstra, explores the unique behaviours and risks that face children, young people, adults, seniors and parents in their online engagements. It identifies the most effective cyber safety strategies to specifically address each age cohort.

Key Findings:

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).

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.

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).

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.

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.

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.

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.

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.

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.

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.

To find out more:

- Read the full report
- Lead author **Amanda Third**, discusses one of the key themes of the report – the importance of digital literacy to cyber safety.

Author: rcrellin

Senior Program Officer, Department of Education and Early Childhood Development