Knowledge, control, and strangers: An analysis of resources for preventing self-generated imagery

The problem

Grooming, child sexual abuse material (CSAM), and sextortion offences have shifted with the convergence of young people and offenders in online spaces, resulting in increased production of self-generated CSAM. Research indicates that young people's internet use is influenced by developmental, cognitive, and social factors, but little has looked into how primary prevention resources for these crimes consider such factors.

Aims

- To gain insight into the ways that primary prevention resources from Australia, New Zealand, the USA, and the UK involving the self-generated aspects of grooming, CSAM, and sextortion align or not with how young people use the internet.
- To explore how the same resources align or not with how offenders use technology.

Methodology

This research thematically analysed 150 primary prevention resources for the above crimes and directed at children, youth, and parents/carers. These were from government, NGO, private, and non-profit organisations, and included pamphlets, PDFs, webpages, and books.

Limitations

This research excluded non-written resources, paid resources, and non-English materials. Therefore, it does not exhaustively reflect the prevention resource landscape.

For the full report, visit the ICMEC Australia website:

www.icmec.org.au

Key findings

- Knowledge was positioned as having power to inherently cultivate safer online behaviour from young people, however this is not necessarily true, as knowledge does not always lead to behaviour change.
- Inconsistent messaging was provided about if and how parents/carers should implement technical controls and rules for internet use, as well as who parents, carers, and young people should understand offenders to be (e.g., strangers, friends, or predators).
- Resources align with some ways in which offenders use technology to initiate contact with young people and transition victims across platforms (e.g., to encrypted communication apps).

Implications and recommendations

Organisations should create primary prevention resources to support, rather than hinder, developmental, cognitive, and social factors influencing young people's internet use, and uplift young people's self-confidence to action advice. For this:

- Resources targeting parents and carers could emphasise age-appropriate online safety rules that consider young people's input and experiences, rather than rigid parental control, to encourage autonomy, independence, and open communication.
- To align with young people's online social behaviours, resources could focus less on restrictive technology and "stranger danger" messaging, and instead teach young people to identify and respond to feelings of uncertainty or discomfort.
- Resources should avoid relying on "stranger danger" messaging and sensationalised categorisations of offenders, because this disregards the relationships/trust that offenders can create with victims, including in the context of manipulation, lying, and/or grooming.
- Organisations could consider identifying how offline child sexual abuse and exploitation prevention initiatives align with developmental, cognitive, and social factors to assess whether they can inform the production of OCSEA prevention initiatives.

Written by Shakira Memorey - Master of Cyber Security (Cyber Criminology) student at the University of Queensland.

Academic supervisor - Dr Jonah Rimer.