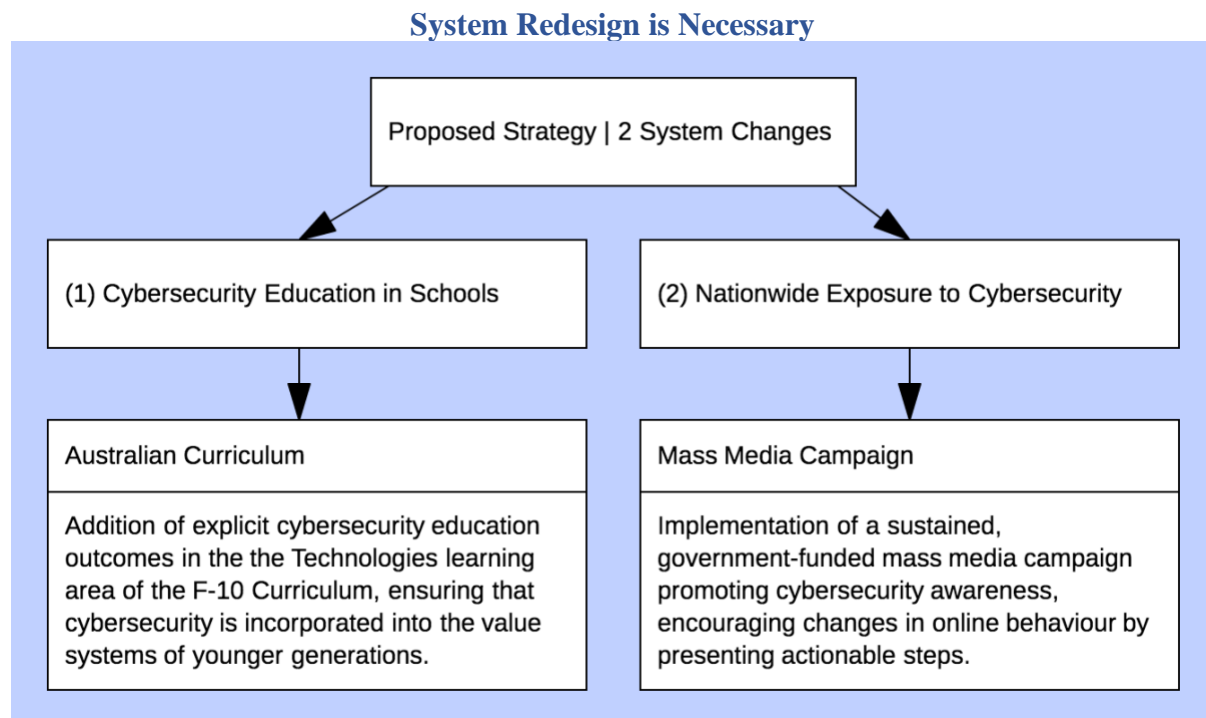


CYBERCRIME PREVENTION THROUGH CYBERSECURITY AWARENESS

Problem: In 2017, approximately 25% of Australians were victims of cybercrime (Australian Cyber Security Centre [ACSC], 2018). Unfortunately, many personal Internet users do not have the necessary cybersecurity awareness to protect themselves against these threats (Kritzinger & Solms, 2010).

Aim: To increase laypersons' cybersecurity awareness, measurable by reductions in personal cybercrime reports to the ACSC.



Justifications:

- (1) The Australian Curriculum does not include cybersecurity learning outcomes: Foundation to Year 10 students are not explicitly taught about cybersecurity (Australian Curriculum, 2015).
- (2) Australian governments' cybersecurity awareness initiatives are limited because they are targeted towards cybercrime victims and interested individuals only (Attorney-General's Department, 2013).

Evidence from Multiple Perspectives

(1) Cyber Security Education in Schools

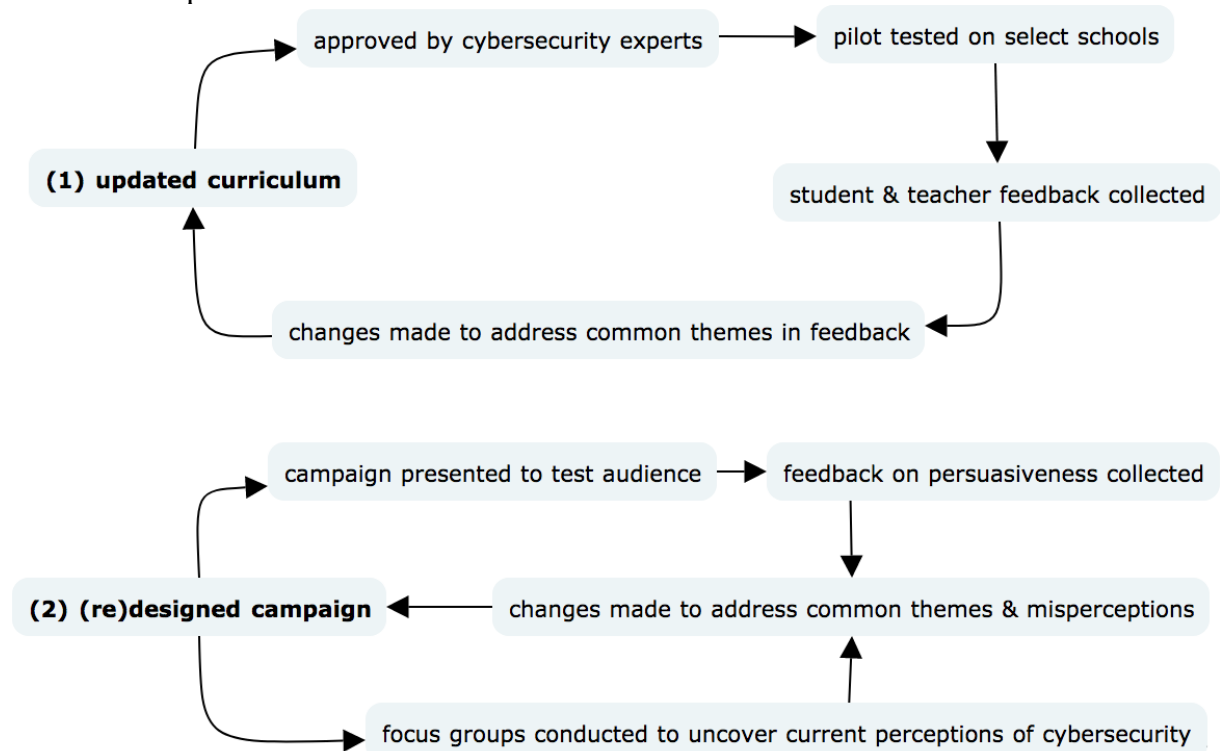
- School-based interventions have effectively increased condom use (Denford, Abraham, Campbell, & Busse, 2017), suggesting that school-based learning has the potential to increase childrens' cybersecurity awareness.
- Joanne Orlando, educational technology researcher, proposed that cybersecurity should be in school curriculums to ensure children understand cyberspace threats (Orlando, 2019).
- Social Cognitive Theory (SCT), which emphasises the role of social context in learning, indicates that children are socialised to accept societal values within school settings (Schunk, 2012). Thus, school-based promotion of cybersecurity awareness should be highly effective.

(1) Nationwide Exposure to Cybersecurity

- The efficacy of mass media campaigns has been corroborated by a recent scientific review of numerous mass media campaigns (Stead et al., 2019). It revealed that sustained mass media campaigns can positively influence a variety of health behaviours across large populations.
- According to SCT, behaviour change is dependent on self-efficacy (belief in one's ability to achieve; Anderson, 2000). Videos containing step-by-step instructions, encouragement, and actors performing target behaviours appear to increase self-efficacy in relation to the target behaviour (Anderson, 2000). Thus, mass media campaigns with similar features should increase cybersecurity self-efficacy, resulting in improved cybersecurity practices.
- Examples of successful Australian mass media campaigns: From 1987 to 2002, 11,589 Victorian adults were surveyed about their sun-safe behaviours (Dobbinson et al., 2008). The research shows that, since 1988, Victoria's ongoing campaign for public awareness of sun safety (SunSmart) has been effective in increasing sun-safe attitudes and behaviours. The SunSmart campaign is a relevant model for a cybersecurity awareness campaign because it targets habitual and ongoing problem behaviours. Further, the success of the National Tobacco Campaign indicates that it should also be used as a model for a cybersecurity awareness campaign.

Early strategy ideas should be iteratively tested and refined.

This iterative process is illustrated below:



Future Threats and Opportunities

The nature of cybercrime is ever-changing, so school curriculums and mass media campaigns inevitably become obsolete. Continuous liaising with cybersecurity experts can help ensure that cybersecurity practices taught in schools and perpetuated through mass media campaigns are relevant to current threats. Nevertheless, the proposed strategy should cultivate public awareness of cybersecurity, which is currently severely lacking. While cybercrime is unpredictable, this strategy ensures it is instilled in public consciousness, which should

naturally reduce cybercrime rates and increase concern as threats arise. Thus, this strategy produces a self-evolving system, responding to cyberspace changes in a dynamic, top-down, and bottom-up way.

Conclusion

Australia's 2020 Cyber Security Strategy acknowledges laypersons' overwhelming lack of cybersecurity awareness but does not propose effective systems to promote safer online behaviour. Australia's Cyber Security Strategy needs to place more emphasis on increasing cybersecurity awareness so that personal Internet users can start to take more control of their digital identity.

References

- Anderson, R. B. (2000). Vicarious and persuasive influences on efficacy expectations and intentions to perform breast self-examination. *Public Relations Review*, 26(1), 97-114. [https://doi.org/10.1016/S0363-8111\(00\)00033-3](https://doi.org/10.1016/S0363-8111(00)00033-3)
- Attorney-General's Department. (2013). *National Plan to Combat Cybercrime*. Retrieved October 6, 2019, from https://www.homeaffairs.gov.au/criminal_justice/files/national-plan-combat-cybercrime.pdf
- Australian Curriculum. (2015). *Digital technologies: Sequence of content*. Retrieved October 6, 2019, from https://docs.acara.edu.au/resources/Digital_Technologies__Sequence_of_content.pdf
- Australian Cyber Security Centre. (2018, November). *One in four Australians hit by cybercrime – reversing the threat*. Retrieved October 6, 2019, from <https://www.cyber.gov.au/news/sso-launch>
- Denford, S., Abraham, C., Campbell, R., & Busse, H. (2017). A comprehensive review of reviews of school-based interventions to improve sexual-health. *Health psychology review*, 11(1), 33-52. <https://doi.org/10.1080/17437199.2016.1240625>
- Dobbinson, S. J., Wakefield, M. A., Jansen, K. M., Herd, N. L., Spittal, M. J., Lipscomb, J. E., & Hill, D. J. (2008). Weekend sun protection and sunburn in Australia: trends (1987–2002) and association with SunSmart television advertising. *American journal of preventive medicine*, 34(2), 94-101. <https://doi.org/10.1016/j.amepre.2007.09.024>
- Kritzinger, E., & Solms, S. (2010). Cyber security for home users: A new way of protection through awareness enforcement. *Computers & Security*, 29(8), 840-847. <https://doi.org/10.1016/j.cose.2010.08.001>
- Orlando, J. (2019, February 26). Kids need to learn about cybersecurity, but teachers only have so much time in the day. *The Conversation*. Retrieved October 10, 2019, from <https://theconversation.com/kids-need-to-learn-about-cybersecurity-but-teachers-only-have-so-much-time-in-the-day-112136>
- Schunk, D. H. (2012). Social cognitive theory. In K. R. Harris, S. Graham, T. Urdan, C. B. McCormick, G. M. Sinatra, & J. Sweller (Eds.), *APA educational psychology handbook, Vol. 1. Theories, constructs, and critical issues* (pp. 101-123). Washington, DC, US: American Psychological Association. <http://dx.doi.org/10.1037/13273-005>
- Stead, M., Angus, K., Langley, T., Katikireddi, S. V., Hinds, K., Hilton, S., Lewis, S., Thomas, J., Campbell, M., Young, B., & Bauld, L. (2019). Mass media to communicate public health messages in six health topic areas: A systematic review and other reviews of the evidence. *Public Health Research*. <https://doi.org/10.3310/phr07080>