Laura M Saxton

LCYS_2022

CDF 1

Summary Post

While the extortion of users on social media is continuously on the rise, exploitation of children on these platforms has “risen steeply in the last decade” (Al Habsi et al., 2021: 527). Facebook is a apt example of this, as default settings on the app “allow profiles to be too open and publicly viewable” (Alkawaz et al., 2020: 142), exposing unsuspecting users to spear-fishing attempts through external link offers or the collection of sensitive information through private chats (Anderson, 2020).

However, implementing security protocols to prevent blackmail on social media sites is not a straightforward task. Firstly, the question of responsibility is somewhat contentious. Users “look to both organizational policies and governmental regulations to safeguard their online privacy” (Lwin et al., 2007: 583), while companies tend to “claim status as a neutral intermediary” (Wildenauer, 2020: 3), reaping the benefits of online activity without taking on liability.

While acting as an intermediary is perhaps an accurate description of the social media company’s role, this should not preclude culpability if crimes are being carried out on their platforms; especially if such crimes include the abuse of children and adolescents. At minimum, these companies should encourage responsible sharing of information between users.

There are a number of ways such could be carried out, and implementation would depend on the jurisdiction and use requirements of each application (GDPR, 2016; NIST, 2012; Anderson, 2020), but it may be prudent to restrict more sensitive interface features from those under a certain age. In tandem, users should be encouraged to take personal responsibility. It is not enough for companies to warn users about privacy risk if those warnings go unheeded. As Xue Ling Teh has noted, security education “ought to start from the bottom-up” (2022), and be incorporated into the cultural lexicon.

Securing privacy online need not be the sole responsibility of a company or user. It could be a shared endeavor, with special attention paid towards preventing the exploitation of underage individuals, at both top-down and bottom-up levels.

References

Al Habsi, A., Butler, M., Percy, A. and Sezer, S., 2020. Blackmail on social media: what do we know and what remains unknown?. *Security Journal*, [online] 34(3), pp.525-540. Available at: https://eds.s.ebscohost.com/eds/detail/detail?vid=2&sid=7c9e409e-c419-4086-80a9-b644793fc845%40redis&bdata=JnNpdGU9ZWRzLWxpdmU%3d#AN=edssjs.CC5FA32D&db=edssjs [Accessed 19 June 2022].

Alkawaz, M., Abdullah, M. and Rajandran, H., 2020. The Impact of Current Relation between Facebook Utilization and E-Stalking towards Users Privacy. In: *2020 IEEE International Conference on Automatic Control and Intelligent Systems (I2CACIS 2020)*. [online] Available at: https://0-ieeexplore-ieee-org.serlib0.essex.ac.uk/stamp/stamp.jsp?tp=&arnumber=9140098 [Accessed 19 June 2022].

Anderson, R., 2020. *Security Engineering: A Guide to Building Dependable Distributed Systems*. 3rd ed. Indianapolis, USA: Wiley.

European Parliament, 2016. General Data Protection Regulation.

Lwin, M., Wirtz, J. and Williams, J., 2007. Consumer online privacy concerns and responses: a power–responsibility equilibrium perspective. *Journal of the Academy of Marketing Science*, [online] 35(4), pp.572-585. Available at: https://link.springer.com/content/pdf/10.1007/s11747-006-0003-3.pdf [Accessed 3 July 2022].

National Institute of Standards and Technology, 2012. Computer Security Incident Handling Guide.

Teh, X. L., 2022. Peer Response -- Xue Ling Teh. [Blog] *Re: Initial Post -- Laura Saxton*, Available at: https://www.my-course.co.uk/mod/forum/discuss.php?d=112494 [Accessed 3 July 2022].

Wildenauer, M., 2020. The Shared Responsibility Model: Levers of Influence and Loci of Control to aid Regulation of Ethical Behaviour in Technology Platform Companies. *Australasian Journal of Information Systems*, [online] 24, pp.1-21. Available at: https://journal.acs.org.au/index.php/ajis/article/download/2797/977/ [Accessed 3 July 2022].