

Security and Privacy Challenges with Shared Digital Identity and Devices in urban Northern Territory Aboriginal Communities

This study explored the security and privacy challenges experienced by the Australia's Northern Territory Aboriginal urban communities in living their culture that believes in sharing their digital identities and devices. Preliminary findings have confirmed that sharing of devices and digital identities was occurring and that victimisation occurs when motivated offenders will act upon opportunities when they encounter suitable targets that lack capable guardianship. The study represents a first attempt to recognise the Indigenous voice in the design of cybersecurity frameworks, policies, and procedures. There is need for a shared security objective and joint design of frameworks, policies and procedures between the guardian institutions, the service providers, and the user community.

Abstract

This research study explored the security and privacy challenges experienced by the Australia's Northern Territory Aboriginal urban communities in living their culture that believes in sharing, including their digital identities and devices. The study adopted the routine activity theory (RAT) to understand and explain the victimisation risks associated with the sharing of digital identities and devices. RAT states that motivated offenders will act upon opportunities when they encounter suitable targets that lack capable guardianship. The research adopted an Indigenous research methodology involving Indigenous peoples applying their own worldview, perspectives, and understandings. Interviews were conducted with Indigenous community participants in the Darwin area of the Northern Territory of Australia. The interview sessions collected data about their views on sharing devices and digital identities and captured their cultural perspectives and understanding of cyber security risks. Preliminary findings have confirmed that sharing of devices and digital identities was occurring in the Darwin Indigenous communities. The preliminary findings support the routine activity theory that victimisation of the communities will occur because offenders will take advantage of risk occurring due to the sharing of digital identities and devices. increases the opportunities for motivated offenders as it exposes them for targeting by cybercriminals. Based on these findings, a shared security design model that embraces the Indigenous culture and participation is recommended.