PHYS.ORG

Aboriginal communities embrace technology, but they have unique cyber safety challenges

November 29 2016, by Ellie Rennie And Tyson Yunkaporta

For many people living in remote Aboriginal communities, mobile devices are the sole means of accessing the internet. However, when the use of mobile devices oversteps social and cultural lines, it can have serious consequences for individuals and their families.

While some people avoid social media and online financial transactions as a protective measure, this can result in new forms of digital exclusion.

Our research into online risks, carried out in central Australia and Cape York, reveals unique problems in remote communities, many of which are caused by the sharing of devices.

For instance, some young people are using others' social media accounts to deliberately overstep cultural authority. Borrowing or taking someone's phone and transferring credit to another phone without permission is also causing financial hardship, particularly for older people.

The sharing of devices leads to insecure banking, causing some to avoid online banking and Centrelink accounts altogether. It can also mean that text messages are received by people they were not intended for, leading some people to smash phones or destroy SIM cards.

Consequences

The consequences of social media communication can be serious in a remote Aboriginal community.

For instance, a young person using someone else's social media account without the owner's permission might exacerbate existing inter-family tensions. This can cause conflicts to spread from a group of teens to their adult relatives, causing a "wildfire" of community fights.

Acts that might seem benign in other contexts, like flirting through a dating site, can breach cultural law ("wrong way" relationships), resulting in ostracism with mental health consequences.

Aboriginal people have systems for dealing with offline transgressions before they get out of hand. But authority lines may not work where communication is across multiple communities or if elders are absent from social media platforms.

In places where authority is already diminished, unsanctioned acts of recompense can make cyber safety an issue of immediate safety.

Individual protective measures against device theft and account hacking, such as concealing devices in clothing, may ensure cyber safety on one level. But these can also be damaging to kinship relationships as traditional routines of exchange and sharing practices are disrupted.

Community leaders and groups are experimenting with extraordinary measures, including switching off public Wi-Fi hotspots when cyber-bullying incidents threaten to escalate into community violence. Some communities have refused mobile infrastructure altogether.

Solutions

While the advent of mobile telephony in remote areas may be creating new problems, mobile phones and internet access are important. Social media is connecting families across vast distances, including with relatives needing to live in town for education or medical reasons.

In the absence of home telephones and internet, mobile phones are often the only means for individuals to access online services, such as e-government sites and internet banking.

Empowering people to use applications such as internet banking could also help overcome the kind of exploitation revealed through the "book up" theft in Mintabie, South Australia, in which A$1 million was stolen from local Aboriginal people's bank accounts by a store keeper.

Paying attention to how different groups use technology can assist in determining how device and platform features evolve in ways that suit everyone.

We found that older people in remote communities and towns need assistance to learn how to set passwords, block people from social media and avoid scams.

However, we are finding that while simple security measures can make a big difference, they are not always failsafe.

"Find my phone" apps can be useful for when a device is "borrowed" and not returned, but the user will need access to a second device to track the first.

Biometric security may assist people to keep their phones from being used by others, but PINs and passwords can generally override these measures, and social pressure to share passwords can mitigate device security.

Further technological measures, such as filtering certain sites, or instituting a "kill switch" on a Wi-Fi network when tensions arise may give the community control, but are not likely to be accepted in larger towns where businesses and tourists rely on and expect internet freedoms.

Finally, we found that the term "cyber safety" is not necessarily recognised in remote communities. Instead, the word for "protection" is favoured, which suggests a far more pro-active set of behaviours, including a social obligation to watch out not only for oneself but for the entire social and family group as well.

While this obligation to defend each other can sometimes escalate instances of online violence in remote communities, it also demands an active rather than passive approach to online risks, a collaboratively defensive attitude that may be key to communities developing their own responses.

This article was originally published on The Conversation. Read the original article.

Provided by The Conversation

Citation: Aboriginal communities embrace technology, but they have unique cyber safety challenges (2016, November 29) retrieved 18 July 2024 from https://phys.org/news/2016-11-aboriginal-embrace-technology-unique-cyber.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.