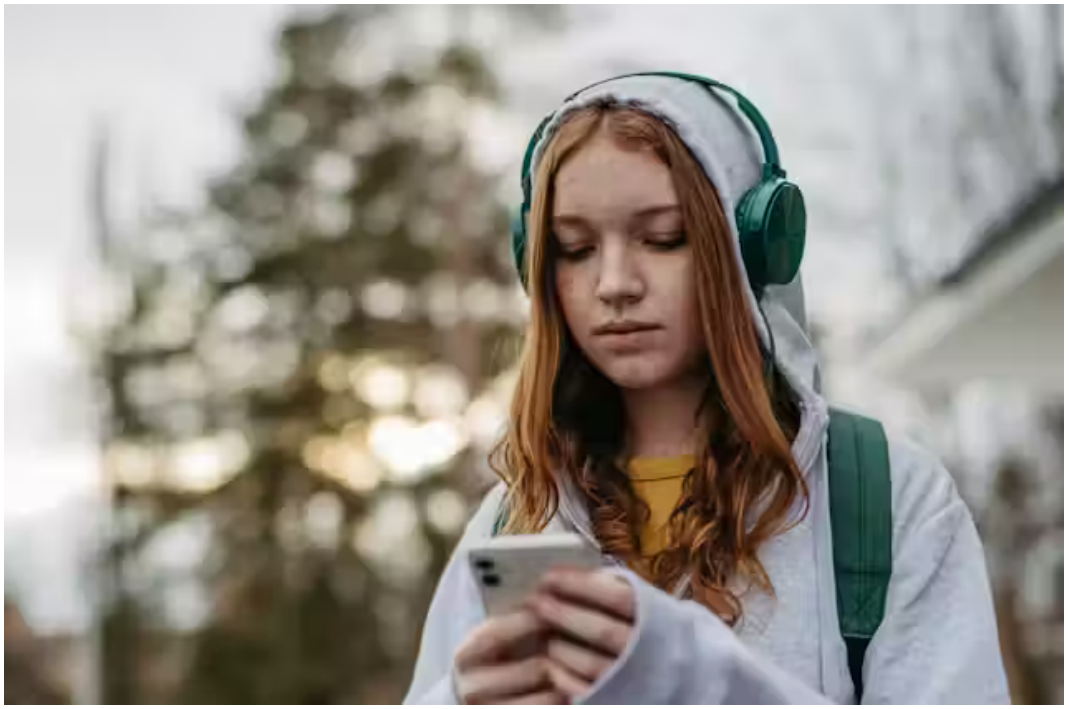
THE CONVERSATION

Academic rigour, journalistic flair



Halfpoint/ Shutterstock , CC BY

91% of Australian teens have a phone – but many are not keeping their identity and location secure

Published: September 9, 2024 6.23am AEST

Yeslam Al-Saggaf
Professor in Computing, Charles Sturt University

Julie Maclean
Researcher in Computing, Charles Sturt University

Most Australian teenagers have their own smartphone. According to a 2023 survey, 91% of young people between 14 and 17 owned a phone.

At the same time, there is huge community concern about young people being exposed to harms online – this includes the content they consume and the interactions they might have.

But there is also concern about their privacy and security. A 2023 UK study found teenagers are overly optimistic about the degree to which they can protect their personal information online.

This is a problem because smartphones can communicate information such as identities and locations when settings are not figured correctly.

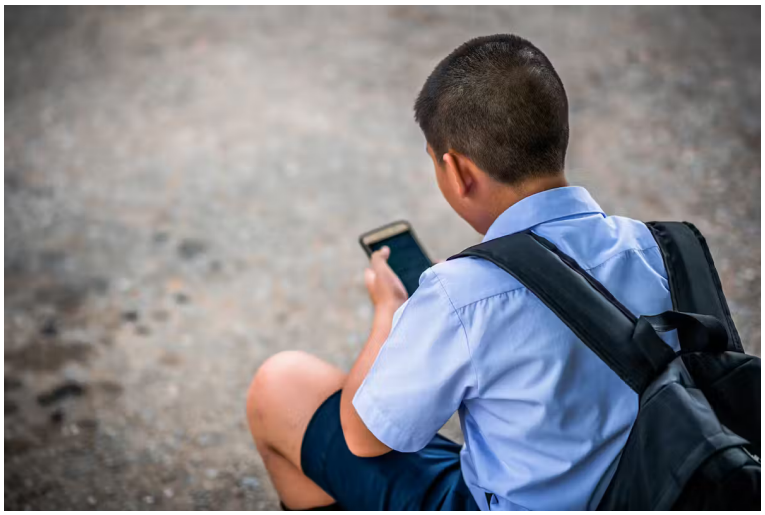
Our new project – which has been funded by the eSafety Commissioner and will soon be available online – looked at how to teach students to be safer with their phones.

What are the risks?

Without changing the default settings, a phone (or smart watch, laptop or tablet) can share information such as full names, current locations and the duration of their stay in those locations. This makes it easy for others with basic IT knowledge to create profiles of someone's movements over time.

Children are at particular risk, as they often connect to free public Wi-Fi networks. They may also be more likely to exchange photos with strangers online and accept social media friend requests without caution.

This also puts them at increased risk of having their identity or money stolen or coming into contact with people who may wish them harm.



It is easy to give away your identity and location if your phone is not set up securely. POP-THAILAND/ Shutterstock, CC BY

Our research

Our project was conducted in seven high schools in regional New South Wales between August 2023 and April 2024.

First, we set up network sensors in two schools to monitor data leakage from students' phones. We wanted to know the extent to which they were they giving away names and locations of the students. This was conducted over several weeks to establish a baseline for their typical data leakage levels.

Next, we gave 4,460 students in seven high schools lessons in how smartphones can leak sensitive information and how to stop this. The students were shown how to turn off their Bluetooth and switch off their Wi-Fi. They were also shown how to change their Bluetooth name and switch off their location services.

We then measured data leakage after the lesson in the two schools with network sensors.

We also conducted a survey on 574 students across five other schools, to measure their knowledge before and after the lesson. Of this group, about 90% of students owned a smartphone and most were aged between 14 and 16.

What did we find?

We found a significant reduction in data leakage after students were given the lessons.

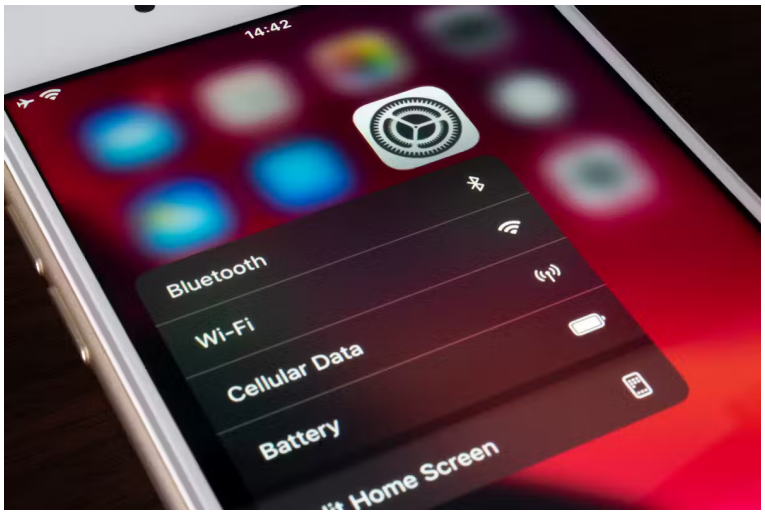
At the two schools we monitored, we found the number of identifiable phones fell by about 30% after the education session.

The survey results also indicated the lessons had been effective. There was an 85% improvement in students' "knowledge of smartphone settings" questions.

There was also a 15% improvement in students' use of a safer, fake name as their smartphone name after the lessons – for example, instead of "Joshua's phone", calling it "cool dude".

There was a 7% increase in concern about someone knowing where they were at a particular point in time, and a 10% increase in concern about someone knowing what their regular travel route to school was.

However, despite their enhanced understanding, many students continued to keep their Wi-Fi and Bluetooth settings enabled all the time, as this gave them convenient access to school and home Wi-Fi networks and headphone connections. This is an example of the "privacy paradox" where individuals prioritise convenience over security, even when aware of the risks.



Our study found education sessions can improve the way teenage students use their phones. PSGflash/Shutterstock, CC BY

How can students keep their phones safe?

There are three things young people – and others – can do to keep their smartphones safe.

1. Switch off services you don't use

Phone owners should ask themselves: do I really need to keep all the available services on? If they are not using Wi-Fi, Bluetooth or location services (such as Snap Map, where you share your location with friends), they should turn them off.

As our research indicated, young people are unlikely to do this because it is inconvenient. Many young people want to connect to their headphones at all times so they can listen to music, watch videos and talk to friends.

2. Hide the device

If teens can't switch off these services, they can at least de-identify their device by replacing their real name on the phone with something else. They can use a name parents and friends will recognise but will not link them to their other data.

They can also hide their device by not giving away the type of phone they are using (this can be done in general settings). This will prevent cyber attackers from linking their phone to the security vulnerabilities with their make of phone.

3. Control each app

Ideally, students should also go in and check smartphone settings for individual apps as well – and turn off services for apps that don't require them. It is now easy to find out which apps have access to location services and your phone's camera or microphone.