What Parents & Carers Need to Know About

SIGNAL

12+ App Store Rating

Signal is a multimedia messaging service (previously known as TextSecure) which provides secure chats between users. It is encrypted, so any intercepted communication cannot be read by attackers. Users can send one-to-one messages or set up group chats. The service is free, has no adverts and doesn't track users' location like many other messaging platforms. The app experienced a popularity boom in early 2021 as large numbers of users left WhatsApp over perceived privacy issues.

Disappearing Messages

Messages on Signal can be set to disappear (from both the sender and the recipient's devices) a specified time after they are first opened – potentially as little as five seconds. So it is difficult to monitor the app and see what your child is talking about. Should someone behave inappropriately towards them, unless they record evidence instantly there is no way to prove what has happened – making it difficult to take the proper action.

False Sense of Security

The feeling of total privacy and security within the app can make young people feel like they are invulnerable – and possibly that they could get away with behaving in ways they normally wouldn't. This behaviour could range from the harmful (such as participating in cyber bullying or sharing age-inappropriate images or videos) to the extremely dangerous: perhaps chatting to strangers, who might potentially be predators.

Risk of Screengrabs

Because messages can be set to disappear on Signal, some young people assume that nobody else will ever see them and let their guard down as a result. But a recipient could still capture a screenshot of your child's message before it vanishes from their device. This screengrab – which might be of something inappropriate or deeply personal – can then be shared with others or even made public on the internet.

Vulnerability to Hackers

Like virtually any piece of software, Signal has been shown to have flaws in its security. One hacker was able to make a call to a target device using the app and could then listen in on the victim through their phone – without needing them to even answer the call. Afterwards, the hacked user was completely unaware that the eavesdropping had taken place.

Advice for Parents & Carers

Gather Any Evidence Quickly

If your children are old enough to use Signal, they will likely already know how to take a quick screenshot on their phone. It's best to confirm this with them, however, because if they're sent something inappropriate or offensive, they will only have a very short opportunity to screenshot it as evidence of misconduct before the message disappears. Once they've captured the screenshot, they should then come to you or another trusted adult.

Talk about Online Bullying

Before your child downloads Signal, have an open discussion about the potential risks of this app and others like it. Ensure your child is aware of the possibility of bullying or hurtful messages on such platforms. They should understand that the app makers themselves do not help with investigating incidents – and that it may be difficult to prove someone has done something to upset them.

Think before Sending

The messages a young person sends on Signal don't last forever, but the effects of those messages very well might – for your child and for others. You could suggest to your child that, if they're unsure whether to send a particular message, they should ask themselves if they would be comfortable showing the content to you. And if they wouldn't, should they really be sending it at all?

Stay Updated

It's wise to make sure your child knows how to keep their software up to date by downloading the latest version. Developers will often release software updates that (as well as occasionally adding new features or improving functionality, etc.) help to fix any security flaws and stop hackers from exploiting possible weak points in the app.

Consider Online Reputation

Talk to your child about the implications if a message they sent was made public without their consent. Remind them that once an image (for example) is out there, there's no way to control what happens to it or erase every single copy. It's a good way to get young people to start considering how their digital footprint might have repercussions on their future prospects.

Meet Our Expert

Emma Davis is a cyber security expert and former ICT teacher. She delivers cyber awareness training to organisations nationally and has extensive knowledge and experience of managing how children access services and apps online.

SOURCES: https://smartsocial.com/signal-app/, https://www.signal.org

National Online Safety®

#WakeUpWednesday