What Parents & Educators Need to Know about

APP & PLAY STORES

WHAT ARE THE RISKS?

Since the introduction of Apple's App Store and Google's Play Store, an estimated two million apps have been made available on each. Ofcom's 2025 media use and attitudes report states that more than half of children aged between 3 and 7 use apps or sites to communicate with each other, and, by the ages of 10 to 12, 45% of children are playing games on their mobile phones. This guide will help you ensure that children use the app stores and their content safely.

MALICIOUS APPS WITH MALWARE

Although Google and Apple must approve the apps on their official stores, inappropriate content sometimes slips through the net. For example, in 2025, the security company Kaspersky found that multiple iOS and Android apps contained screen-reading software, primed to look for passwords and stealing crypto-wallet recovery phrases captured in screenshots.

PREDATORY IN-APP PURCHASES

App-making is a business, and most creators have found that 'freemium' software is the way to make money. That means the app will be free initially but will either require the user to watch ads or rely on them making in-app purchases. Some 'free' apps can be predatory, and there are plenty of examples reported where parents have racked up huge bills on behalf of their children's app activity.

UNOFFICIAL COPYCAT APPS

Both official app stores contain copycat apps – often games – designed to look like popular rivals, mimicking their branding, layout and logos. While these will usually just offer a poor experience packed with ads as a quick money-making exercise, they're also more likely to be vessels for malware than the products they're counterfeiting.

ADDICTIVE BY DESIGN

Phone addiction is fast becoming recognised as a real concern, and apps are a big part of this. Freemium apps have a real incentive to keep children checking in every day in order to generate more ad views or secure extra in-app purchases. This can interfere with schoolwork and other offline hobbies.

INAPPROPRIATE CONTENT

As the App Store and Play Store are for all ages, there's a lot of content available that's inappropriate for children. Examples include apps that have references to alcohol, drugs, sex, violence or gambling. In general, these are sensibly age-rated, but social media sites such as YouTube and TikTok, which both have an App Store age rating of 12+, can be gateways to adult material.

SIDELOADED BANNED APPS

'Sideloading' – the more complicated practice of installing applications on a device from sources other than the official app stores – bypasses Google's and Apple's security procedures; however, it is possible for tech-savvy users. This opens up huge risks – not just apps that would be forbidden by Apple and Google, but pirate ones packed with malware too.

Advice for Parents & Educators

ACTIVATE PARENTAL CONTROLS FOR APPS

Both Google and Apple have apps that can give adults greater control over children's phone activity. 'Screen Time' (iPhone) and 'Family Link' (Android) have a range of features, such as letting you set age-related restrictions on the app stores, require permission to download an app, set daily time limits on specific apps, and control real-world spending.

LOOK BEYOND THE REVIEWS

App store reviews are helpful, but they are easily gamed, and some unscrupulous developers will pay for quick reviews to give their work perceived legitimacy. Take more than a cursory glance at listings by digging out the one- and two-star reviews and looking closely at the developer – for example, if they've published a lot of unrelated apps, that's a red flag.

DO YOUR RESEARCH

If children ask permission to download an app, do your due diligence and research it. Read the app summary and search the internet for reviews and discussions to establish its legitimacy, safety and appropriateness – if it doesn't seem to be appropriate, look for safer alternatives instead.

TALK TO YOUR CHILD

Talk to children and make sure they're aware that apps can be risky. As part of a wider talk about internet literacy, ensure they don't download apps outside of the official channels, nor grant apps permission to access their camera, microphone, or photos without a good reason. Make sure they understand that in-game currency costs real-world money.

Meet Our Expert

Alan Martin is an experienced technology journalist who has written for the likes of Wired, TechRadar, The Telegraph, The Evening Standard, The Guardian and The New Statesman.

#WakeUpWednesday® The National College®