At National Online Safety, we believe in empowering parents, carers and trusted adults with the information to hold an informed conversation about online safety with their children, should they feel it is needed. This guide focuses on one of many issues which we believe trusted adults should be aware of. Please visit www.nationalonlinesafety.com for further guides, hints and tips for adults.

What Parents & Carers Need to Know about

SETTING UP APPS, GAMES AND SOFTWARE

Millions of new phones, tablets, laptops and games consoles will be nestling under Christmas trees this year. However, even if parents and carers have gone to the trouble of setting up these new devices and enabling the safety features, there are still potential hazards in the apps, games and software that children will want to install and use. Knowing what to look for and discussing those risks with your child may help avoid any nasty surprises this Christmas. Here are our top tips for ensuring that unwrapping this year's presents doesn't unleash any unexpected dangers.

TAKE NOTE OF AGE RATINGS

Back when most games were bought in shops, checking the age rating was easy: it was on the front of the box. Now that most games are downloaded, it's tougher – but not impossible. All reputable download stores show a game's age rating at the point of purchase, and you can check the suitability of a specific title your child wants to play at videostandards.org.uk/RatingBoard/games.

'FREE' ISN'T ALWAYS FREE

The games market has changed radically in recent years. Many titles are free to download, but then tempt players to pay for cosmetic items (as in Fortnite) or to unlock additional content. There can be huge peer pressure for children to pay for these items. Agree a budget for in-game purchases before the game is downloaded, and make sure children can't authorise in-game purchases by themselves.

DISABLE IN-APP PURCHASING

It's not wise to leave children with devices that can make in-app purchases without your permission. Ideally, set up computers, consoles and phones so child accounts need an adult's authorisation to buy anything. On shared devices (like iPads, which don't allow user accounts), check the settings to ensure that in-app purchasing requires the account holder's password, fingerprint or face ID.

CHECK THE SPECS

To avoid let-downs, check a game's specs before buying – especially for PC or Mac, where games often need a particular graphics chip or processor to work. Sites like systemrequirementslab.com can scan your computer to see if it will run certain games properly. On consoles, make sure you're buying the right version: some newer Xbox or PlayStation games won't play on older consoles.

MONITOR IN-GAME COMMS

Voice chat with friends is part of the fun of modern gaming – but danger lurks here too. Many titles have open chat systems, meaning that children could speak to strangers or hear adult language and verbal abuse when games get particularly competitive. Using a shared family area (as opposed to alone in bedrooms) for online gaming is a good way to keep an occasional ear on what's being said.

BE WARY OF GIFTS

Titles like Roblox, Minecraft and Fortnite have in-game currencies, which can be earned through progress in the game – but can also be bought with real money. A common scam is for a young player to be offered currency if they click a link, visit a certain site or contact another user directly. Warn your child about such offers; they should show you if they're in any doubt over an in-game gift.

APPS ARE AGE RATED, TOO

Like games, apps in the major stores have age ratings, too – so you can see in advance whether an app's appropriate for your child. Additionally, phones' parental control settings allow you to set age limits, preventing young ones from downloading unsuitable apps themselves. These ratings aren't infallible, however: we've seen TV apps featuring adult shows with an age rating of 3, for example.

CONSIDER STORAGE

Most apps and games will tell you in the online store how much space they need on a device. Check this carefully – especially with games, which can run into hundreds of megabytes and beyond. If you don't have enough free storage on a device to run the game or app, you won't get a refund from the store. You can normally check a device's available storage space through the settings menu.

WATCH OUT FOR IMITATORS

Even in the official stores, untrustworthy rogue apps can slip through the net. Common tricks are apps or games that have a slightly different name to the genuine article (Fortnight rather than Fortnite, for instance) or use logos which deliberately look very similar to the official app. To avoid downloading these imitations, read the app's description and check who the publisher is listed as.

LEGAL APPS THAT BREAK THE LAW

There are many apps that are perfectly legal but enable illegal activity – streaming apps which let people watch football matches, say, without paying for Sky or BT Sport. Prosecution for using such apps is rare, but they *can* lead to risky behaviour like viewing rogue streams on sites teeming with malicious links. Watch for children installing unusual apps with 'TV', 'stream' or 'sport' in the name.

IN-APP REGISTRATION

It's common for apps and games to ask users to register: entering personal details like email address, date of birth and other information you might not want your child to divulge. Ask them to get your permission before giving any personal info to an app – and consider using *your* details rather than the child's, so they're not targeted by marketing spam or put at risk of having their data stolen.

STAY UPDATED

Most games and apps are subject to regular updates, which not only offer new content and features but also provide critical security improvements. Children tend to ignore such updates – usually because they don't understand why they're important, or they simply want to get straight on with gaming. Check your child's devices periodically to make sure these updates are being installed.

Meet Our Expert



Barry Collins has been a technology journalist and editor for more than 20 years, working for titles such as the *Sunday Times*, *Which?*, *PC Pro* and *Computeractive*. He's appeared regularly as a technology pundit on television and radio, including on *Newsnight*, Radio 5 Live and *ITV News at Ten*. He has two children and has writes regularly about internet safety issues.

National Online Safety®

#WakeUpWednesday

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 14.12.2022