Millions of new phones, tablets, laptops and games consoles will be nesting 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.

**FREE ISN’T ALWAYS FREE**

The games market has changed radically in recent years. Many titles are free to download, but then charges to pay for cosmetic items (as in Fortnite) or to unlock additional content; there can be huge pressure for children to pay for these items. If you plan to buy 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 before purchasing. If purchasing requires the account holder’s password, fingerprint or face ID.

**APPs ARE AGED, TOO**

Like games, apps in the major stores have age ratings, too - so you can see in advance whether an app is 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 an adult shows with an age rating of 3, for example.

**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 lead to risky behaviour like viewing rogue streams on sites teeming with malicious links. Watch for children installing unusual apps with ‘stream’ or ‘SPORT’ in the name.

**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 space on your 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.

**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, so make sure they understand why they’re important, or they simply won’t get straight onto gaming. Check the app’s store pages to make sure these updates are being installed.

**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. Managers like Steam can scan your computer to see if it will run specific games you can buy. Our consoles make sure you’re buying the right version; some newer Xbox or PlayStation games won’t play on older consoles.

**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 a game key in return for payment. Ask to see the Official website, and check if they’re from the correct country. Many games have different versions for different countries. If they are, the key will be invalid in your country.

**WATCH OUT FOR IMITATORS**

Even in the official stores, untrustworthy rogue apps can slip through the net. Common tricks include games that have a slightly different name to the genuine article (for example, rather than Fortnite or Aliens vs. Predator). Look for the Official app logo, and read the reviews carefully. Ask if a child knows the name of the actual game, and if they know any other players.

**MONITOR IN-GAME COMMUNICATION**

Voice chat with friends is part of the fun for many games, but danger lurks here too. Many titles have a feature that means that children could speak to strangers and sound like you. A common scam is for a young player to be offered a game key in return for payment. Ask to see the Official website, and check if they’re from the correct country. Many games have different versions for different countries. If they are, the key will be invalid in your country.

**TAKENotes OF AGE RATINGS**

Back when most games were bought in stores, checking the age rating was easy thanks to the rating from 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).

**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 Computer Weekly. He’s appeared regularly on technology punditry on television and radio, including on Newsnight, Loose Women and IT News: 2am. He has two children and has written widely about internet safety issues.

**www.nationaonline-safety.com **

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of imprint: 04.12.2021.