Get Safe Online

Get Safe Online is the UK's leading source of information and advice on online safety and security, for the public and small businesses. It is a not-for-profit, public/private sector partnership backed by law enforcement agencies and leading organisations in internet security, banking and retail.

For more information and expert, easy-to-follow, impartial advice on safeguarding yourself, your family, finances, devices and workplace, visit **www.getsafeonline.org**

If you think you've been a victim of online fraud, report it to Action Fraud, the UK's national fraud and cybercrime reporting centre on 0300 123 20 40 or at www.actionfraud.police.uk

GET SAFE ONLINE .org

www.getsafeonline.org

OFFICIAL PARTNERS

TESCO · kaspersky · Gumtree · Standard Life · first direct · M&S BANK · HSBC · Royal Bank of Scotland · NatWest · LLOYDS BANK · HALIFAX · BANK OF SCOTLAND · creativevirtual · ROYAL AIR FORCE · CITY OF LONDON POLICE · NPCC · NATIONAL TRADING STANDARDS eCrime Team · cifas · VICTIM SUPPORT · EUROPOL EC3 · ActionFraud · METROPOLITAN POLICE · Ofcom · neighbourhood ALERT

Fleeceware...

... when "free" does not really mean free

GET SAFE ONLINE .org

www.getsafeonline.org

Fleecewear is the name given to mobile apps which overcharge users for functions or features that are widely available in free or other low-cost alternatives. In fact, they are developed with the sole purpose of doing so. Typically, the apps cater for hobbies such as photography and music, but have also been found in QR code and PDF readers.

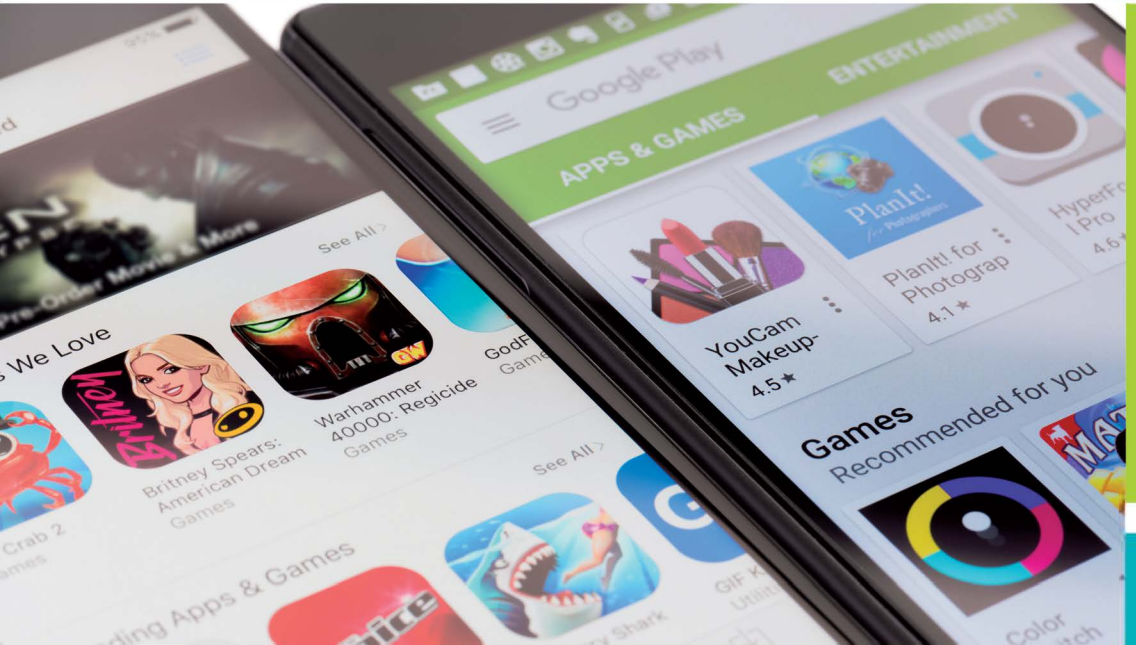
One of our main general tips when advising on downloading apps is to do so only from authorised app stores such as Google's Play Store and Apple's iOS App Store, to avoid your devices being infected with malware. However, an increasing number of fleecewear apps are being found in both stores, as they do not fall into the category of malware, but the grey area of dubious practice.

GET IT ON Google Play

Download on the App Store

Typically, fleecewear apps offer a free trial period, but demand payment following this period, or even the first time they are opened. Alternatively, they request excessive payments for simple features such as photo filters, when these are essential for basic use. Payments can run into thousands of pounds a year, unless cancelled.

The offending app developers find loopholes in the app stores' terms and conditions in order to achieve and maintain listings. They can be found through the stores' search function, but are also frequently advertised on Facebook, Instagram, TikTok, Snapchat and other popular social media platforms. Unscrupulously, developers often target younger audiences through attractive advertisements, themes and promises. Caught up in the moment, children download the apps and the exorbitant payments often continue until significant sums have been taken from the account.



Top tips for avoiding fleecewear

- Don't download the first app that pops up as a result of a search. It may be at the top position through being sponsored by the developer. Compare several apps for features and prices (of both the app and the features).
- Be wary of advertisements for apps on social media platforms and sent to you via email or text of viral advertisements for apps. Those for fleeceware will promise many benefits and be made to seem very attractive.
- Be vigilant when downloading and using applications, to avoid being locked into expensive subscriptions and renewals.
- Be wary of apps that offer free trials of less than a week. Be clear on how much you will be charged after the end of the trial period, and ask yourself if it is worth the money to you.
- As with all purchases and offers, read the small print. The true ongoing price of the app should be included, including the 'in-app purchases' section.
- Ensure it is only you who can pay for apps, and not a child or other unauthorised person. Use the fingerprint or facial recognition confirmation feature on your device, and/or two factor authentication (2FA).

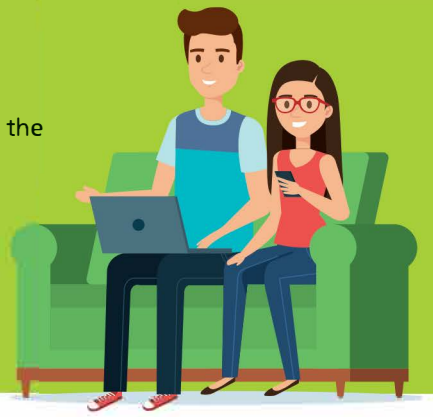
Checking your app subscriptions

For Apple devices, you can either:

- Open Settings, tap your name, then Subscriptions, or
- Open the App Store, touch the icon at the top right of the screen and select Subscriptions.

For Android devices:

- Open Play Store, tap the lined menu icon at the top right of the screen and choose Subscriptions.



Find comprehensive, practical, expert, free advice at **www.getsafeonline.org**