Ashley Junior School

Mr Cousins ICT Systems Manager

Online Safety Newsletter April 2024

Do you need help managing your child's device?

You can use Google Family Link or Apple Family Sharing to help you depending on your child's device.

Google Family Link

This is a parental control app from Google that lets you:

- See activity reports showing how long they spend on each app.
- Approve or block new app downloads.
- Set screen time limits.
- Find their location (using their device).

You will need to download an app and then decide appropriate settings. https://families.google.com/familylink

Apple Family Sharing

You can set up Family Sharing in the settings of your device. Family Sharing allows you to:

- Share Apple subscriptions.
- Share purchases from the App Store.
- Approve what children purchase/download.
- Limit screen time.
- Share locations and find devices.

https://www.apple.com/uk/family-sharing/

Monitoring Apps (paid for)

In addition, there are apps that you can pay for that you may find provides a better solution for you. Whilst we cannot recommend a specific product, these are some examples that you could review and test using a free trial:

- Norton Family: https://uk.norton.com/products/norton-family:
- Qustodio: https://www.qustodio.com/en/

Family Time: https://familytime.io/

Instagram

You will probably know that Instagram is used to post photos and videos, but did you know that it can also be used to message, voice/video call and send disappearing messages? Users can also upload to 'Stories' (which disappear after 24 hours), broadcast live and upload reels (short videos).

You must be over 13 years of age to set up an account. To create an account, you must enter a date of birth (but it is not verified). *When you set up an account for users under 16 years old, the account is set to Private. This is the recommended setting so that your child approves who follows them and sees their content.* Even if your child's profile is private, their bio (at the top of their profile) can still be seen by **everyone.** Check they have not included personal information here e.g. they should not be wearing their school uniform in their photo.

Instagram includes several privacy settings, so go through these with your child and ensure they are set appropriately. Settings include:

- Messages/Group chats – set who can message you/add you to groups.
- Story replies – you can turn this off or choose who can message you.
- Hidden words – turn this option on to hide comments/messages that may be offensive. You can also add your own custom words or emojis.

Make sure your child understands that there is a risk that content they upload can be shared with others without their permission as other users can screenshot it.

Supervision

You can set up supervision on your child's (aged 13-17) Instagram account. This gives you access to a set of tools including the ability to see who they follow/who follows them, how much time they are spending on Instagram, set a time limit and view accounts your child has blocked. Your child can also share when they have reported anything to Instagram with you. Learn more here: https://help.instagram.com/658522825492278

Safety Features

Ensure your child knows how to report posts and people, how to unfollow and block people, delete and turn off comments. View here: https://help.instagram.com/269765046710559

Quiet mode

Your child can activate quiet mode, so they do not receive notifications (to provide less distraction whilst studying and at night time).

How can I keep my child safe on Instagram?

The NSPCC have published a blog with everything that you need to know: https://www.nspcc.org.uk/keeping-children-safe/online-safety/online-safety-blog/keeping-children-safe-on-instagram/

More information

- Visit the family centre to learn more about the features available: https://familycenter.instagram.com/
- Download a parent's guide to Instagram: https://help.instagram.com/299484113584685

What Parents & Educators Need to Know about SHOPPING PLATFORMS

For people looking to make purchases on their phones, several shopping apps – such as Temu – allow users to buy goods at reduced prices. Others, like Vinted and Depop, let you sell items you no longer want. As internet shopping continues to grow, however, so does the risk of scammers, hackers and breaches of privacy.

WHAT ARE THE RISKS?

MISSING ITEMS

Users of Vinted, Depop and Temu have reported not receiving their products despite payment being taken. Users can initially contact the seller to query a missing item, and they have between two and five days (depending on the app) to tell the company what has happened. However, once the money has reached the supposed 'seller', it can be quite difficult to get back.

SCAMMERS AND PHISHING

Scammers are always on the lookout for unsuspecting buyers or sellers. Common tactics include cancelling shipment of an item once the payment has been processed or asking to conclude the chat and payment outside of the app, where the victim is no longer protected by the buyer protection plan. This should, naturally, be avoided at all costs.

DATA MISUSE

Apps of all kinds frequently collect our data, often asking for more information than is necessary to set up an account. Data gathered in this way is then usually sold on to third parties for marketing purposes. Lately, certain apps have been under scrutiny for using spyware to track their members' activities – but all too often, the user's consent to this practice has been hidden away in the terms and conditions.

FAKES OR REPLICAS

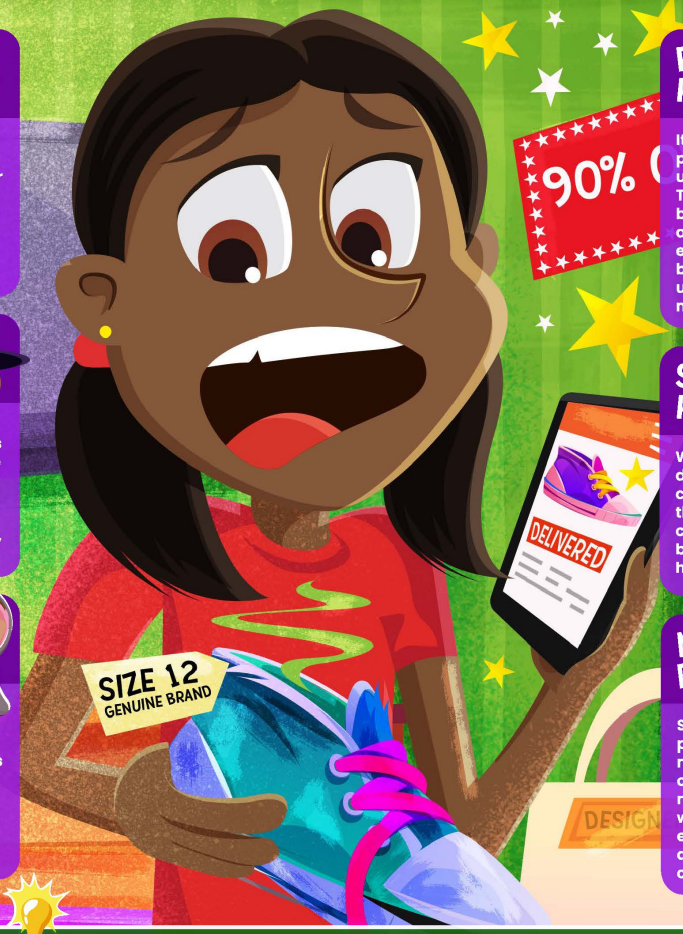
It's certainly not unheard of for poor-quality products to be falsely marketed as luxury items, using misleading pictures or clever wording. These disingenuous sales are sometimes outed by suspiciously low price tags, but this isn't always the case. For children and young people especially, there's a risk that the promise of bagging a high-end item for a fraction of its usual price will outshine any suspicions they may have.

SLOW REFUNDS

While all apps offer a refund if the product is damaged or doesn't match the description, it can take up to a month to be compensated for this. For many people (especially during a cost-of-living crisis) that can be a long time to be without both the product you bought *and* the hard-earned cash you spent on it.

MISLEADING DESCRIPTION

Some people will be able to notice when, say, a product's photo and its description don't seem to match. This isn't a reliable means of picking up on misleading marketing, however – especially not for children and young people, many of whom may not yet realise that such practises even exist. While it's illegal to advertise one thing and sell another, plenty of shady traders use clever wording and omissions to get around this.



Advice for Parents & Educators

ALWAYS STAY ON THE APP

It's vital that users pay for any goods through the same app on which they found them, to ensure they are covered by buyer protection. This means users can access support if the item arrives damaged, isn't as described, or doesn't arrive at all – allowing them to seek compensation for the loss. Such regulations can't protect you, however, if you didn't do the deal through the app in question.

CHECK REVIEWS

Take time to read the reviews and comments left by other users – not just of products, but of sellers and buyers, to ensure they're legitimate and reliable. Before buying an item online, check the reviews for comments about the product's quality, the seller's communication and the delivery time. If you're selling, check the reviews of your buyer for red flags such as frequent requests for refunds or claims of 'missing' items.

BE WARY OF PHISHING ATTEMPTS

Scammers frequently send messages within these apps to steal personal and financial information from other users. Don't respond to these messages – and under no circumstances should you follow any links they contain. Check for spelling errors, as well as inspecting the name of the sender. Report any suspected phishing emails to the app's help centre – and notify your bank if you think your financial information has been compromised.

KEEP SAFE AS A SELLER

Sellers can be exploited just as much as buyers. Some users may purchase an item, for example, then pretend it didn't arrive to secure a refund. Always take photos of the shipping label, along with a picture of you posting the item. Send the package's tracking number to the buyer and keep a copy for yourself, letting you investigate any future claims that it never arrived. When taking photos of items you're selling, ensure nothing personal is in the background.

Meet Our Expert

Dr Claire Sutherland is an online safety consultant at BCyberAware, who has developed and implemented anti-bullying and cyber safety workshops and policies for schools. She has written various academic papers and carried out research for the Australian government comparing internet use and sexting behaviours of young people in the UK, USA and Australia.

Source: See full reference list on guide page at: nationalcollege.com/guides/shopping-apps

#WakeUpWednesday®

The National College®