MOUNT KELLY
Boarding and Day School
Boys and Girls, Aged 4-18

Safeguarding Bulletin

ISSUE 27

Mount Kelly's Safeguarding Bulletin aims to provide parents and carers with the information needed to have informed and age-appropriate conversations with their children about potential risks and issues in the wider world and online. This week's bulletin is on the topics of pop-up ads and shopping platforms.

On the internet or on social media, it's highly likely that you've come across the occasional pop-up – promising a great deal on some product or service, declaring that you've won some kind of prize, or making any other number of tempting claims. This marketing tactic has been around for almost 30 years and shows no signs of disappearing any time soon.

Unfortunately, pop-up advertising carries with it various online safety risks, as we can never be certain where those links will take us or how legitimate their creators are. These ads can be especially risky for children and young people, who may not yet be able to look at such marketing with a critical eye. However, the first of this week's **#WakeUpWednesday** guides will educate you on pop-ups, their associated risks, and how to safeguard yourself and young people from this phenomenon.

Long gone are the days where eBay and Amazon were the only means of buying quality items online. The rise of user-friendly, accessible shopping apps has meant that getting clothes, gadgets and other goodies delivered direct to your door can be accomplished with a few touches of your phone's screen while you're on the go.

These apps aren't without their issues, however, and users still run the risk of scams, data breaches and other online safety concerns. Being aware of these dangers will go a long way to keeping your money and information safe, so you can still enjoy what these shopping apps have to offer. The second of this week's guides has some top tips to help protect young people on these purchasing platforms.

At The National College, our WakeUpWednesday guides empower and equip parents, carers and educators with the confidence and practical skills to be able to have informed and age-appropriate conversations with children about online safety, mental health and wellbeing, and climate change. Formerly delivered by National Online Safety, these guides now address wider topics and themes. For further guides, hints and tips, please visit nationalcollege.com.

What Parents & Educators Need to Know about POP-UP ADS

Pop-up advertisements have been a staple of the internet since they were first introduced in the late 1990s. This form of advertising causes a small window or banner to appear in the foreground while someone is browsing a website. Although these adverts are merely irritating for most people, pop-ups can present more severe risks to younger users.

WHAT ARE THE RISKS?

DECEPTIVE TACTICS

Children sometimes don't understand that adverts (including pop-ups) are designed to sell a product – and can't distinguish between a legitimate feature of a site and an advertisement. Video games, for example, can be full of pop-up ads that tempt users into spending money, yet they might take the form of a mini-game or extra level.

INAPPROPRIATE CONTENT

While some adverts are targeted based on a user's interests and activity online, that isn't always the case. This means that children may unfortunately be exposed to ads for age-inappropriate goods or services such as tobacco products, alcohol and gambling sites.

MALWARE RISK

Most pop-ups from reputable advertisers are safe. However, in some cases, pop-ups can trick you into downloading malware – whereby cybercriminals install software on your device, allowing them to access your sensitive data. It can be difficult to know if malware has been installed on your device, so your best option is to avoid engaging with these pop-ups altogether. Be wary of sites that suddenly bombard you with ads or try to prevent you from leaving.

PRIVACY RISK

Many app and game developers will collect their users' personal data, such as their name, address, email address, geolocation information, unique numerical identifiers, photos and payment information. If a child clicks on an illegitimate pop-up laced with malware, all this information could be put at risk.

RACKING UP BILLS

If a child has access to a payment card on their device – be it a smartphone, laptop, or tablet – they could very quickly rack up a massive bill by interacting with pop-up adverts and buying products shown to them. Try to keep a close eye on their spending.

BEHAVIOURAL IMPACT

Research has found that pop-up ads can even have an impact on children's behaviour. Some of these adverts use manipulative tactics that take advantage of children's developmental vulnerabilities, intentionally or otherwise. This approach may cause a child's mood to shift: becoming more stubborn, for example, if they begin wanting their parents to buy a specific product for them.

Advice for Parents & Educators

START A CONVERSATION

It's important to have regular conversations with children about online advertising so that they understand the risks of interacting with pop-ups. For example, if a child asks for a product which has been advertised to them online, ask them why they want it and how they found it: this will present an opportunity to talk youngsters through the tactics used in online marketing.

SPOT THE SIGNS

If you're concerned that a child may be following pop-up ads to make online purchases or viewing content that could be harmful, it's important to be able to spot the signs. Due to the often-manipulative nature of these adverts, children who interact with them regularly may show signs of distraction, stubbornness and an increasingly materialistic worldview.

MONITOR CONTENT

It can often be difficult to spot when a pop-up advert is malicious – even more so for impressionable younger users. It's important to monitor the content they're consuming to prevent them from clicking on something dangerous. If a pop-up ad seems too good be true – promising a free iPad, for example – it probably is.

PRIVACY SETTINGS

Most modern devices have privacy settings that let you limit the amount of advertising a child is subjected to while using apps or browsing the internet. You may also want to speak to schools about avoiding sites and apps with advertising, as well as adjusting digital privacy settings on any education technology they use.

LIMIT SPENDING

Try to stay aware of what children are spending and ensure that payment details aren't linked to or saved on the gaming platform that they use. Most video games and internet-enabled devices have settings that can help you manage what children can or cannot purchase online.

CUT DOWN ON SCREEN TIME

Given the prevalence of pop-up ads (which can appear on everything from smartphones and tablets to internet-connected toys and games), it might be beneficial to limit the time children spend on digital devices to curb their exposure to digital advertising.

Meet Our Expert

Carly Page is an experienced technology writer with more than 10 years in the industry. Previously the editor of tech tabloid The Inquirer, she is now a freelance technology journalist, editor and consultant who writes for Forbes, TechRadar and Wired, among others.

#WakeUpWednesday®

The National College®

Source: See full reference list on guide page at: https://nationalcollege.com/guides/pop-ups

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 29.05.2024

At The National College, our WakeUpWednesday guides empower and equip parents, carers and educators with the confidence and practical skills to be able to have informed and age-appropriate conversations with children about online safety, mental health and wellbeing, and climate change. Formerly delivered by National Online Safety, these guides now address wider topics and themes. For further guides, hints and tips, please visit nationalcollege.com.

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.

Oscar your password needs changing on your account click the link below.

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.

#WakeUpWednesday®

The National College®

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

@wake_up_weds /wuw.thenationalcollege @wake.up.wednesday @wake.up.weds

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 24.04.2024