National Online Safety®

PARENTAL GUIDE ON POPULAR APPS VISITED BY CHILDREN

NATIONAL ONLINE SAFETY APP ALSO AVAILABLE TO DOWNLOAD

Download today via the relevant app store link below

GET IT ON Google Play

Download on the App Store

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

ONLINE CONTENT

10 tips to keep your children safe online

The internet has transformed the ability to access content. Many apps that children use are dependent on user-generated content which can encourage freedom of expression, imagination and creativity. However, due to the sheer volume uploaded every day, it can be difficult for platforms to regulate and moderate everything, which means that disturbing or distressing images, videos or audio clips can slip through the net. That's why we've created this guide to provide parents and carers with some useful tips on keeping children safe online.

1 MONITOR VIEWING HABITS

Whilst most apps have moderation tools, inappropriate content can still slip through the net.

2 CHECK ONLINE CONTENT

Understand what's being shared or what seems to be 'trending' at the moment.

3 CHECK AGE-RATINGS

Make sure they are old enough to use the app and meet the recommended age-limit.

4 CHANGE PRIVACY SETTINGS

Make accounts private and set content filters and parental controls where possible.

5 SPEND TIME ON THE APP

Get used to how apps work, what content is available and what your child likes to watch.

6 LET CHILDREN KNOW YOU'RE THERE

Ensure they know that there is support and advice available to them if they need it.

7 ENCOURAGE CRITICAL THINKING

Talk about what people might post online and why some posts could cause distress.

8 LEARN HOW TO REPORT & BLOCK

Always make sure that children know how to use the reporting tools on social media apps.

9 KEEP AN OPEN DIALOGUE

If a child sees distressing material online; listen to their concerns, empathise and offer reassurance.

10 SEEK FURTHER SUPPORT

If a child has been affected by something they've seen online, seek support from your school's safeguarding lead.

National Online Safety®

#WakeUpWednesday

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 app of many which we believe trusted adults should be aware of. Please visit www.nationalonlinesafety.com for further guides, hints and tips for adults.

What Parents Need to Know about SQUID GAME

AGE RESTRICTION
15+
Suitable only for 15 years and over.

With themes of horror and violence, it's important for parents and carers to understand the potential risks posed for young audiences by the viral TV show, Squid Game. The nine-episode Netflix-exclusive TV show is rated 15+ and is about a world where contestants who are deeply in debt play children's games in order to win cash prizes. The losers, however, are violently killed. The show's popularity has meant it has spread across online platforms, and there is a great risk of young people being exposed to unsuitable scenes, meaning parents and carers have to be vigilant when allowing children to use devices.

INAPPROPRIATE CONTENT

Some might argue that Squid Game contains content that might not even be suitable for older teens, let alone young children. Characters are brutally tortured and killed through stabbings or getting shot as a result of rules developed and enforced by a masked game master. The show also features sexual content and threats of sexual violence, as well as a strong theme of gambling that runs throughout the whole show.

APPEAL TO YOUNG PEOPLE

Whilst the content is very much adult-themed, some features of the show seem to appeal to young children at face-value. The name "Squid Game" may be interpreted as a programme aimed at children rather than adults. The content itself, such as the bright and childish aesthetics, may also appeal to young children, particularly as there's a focus on playground games to go with it.

SIMILAR CONTENT SUGGESTIONS

When using social media and streaming sites, content is recommended based on what is the user has consumed i.e. what they have watched or searched for. Therefore, there is a greater chance of your child being exposed to similar violent or horror-themed content on social media after watching a show like Squid Game.

VIRAL SPIN-OFFS

As well as Netflix, Squid Game has grown in notoriety and prevalence on other platforms, like TikTok and YouTube, with clips of the show going viral. On YouTube Kids, a number of successful channels have taken advantage of the Squid Game trend, creating content such as "How to Draw Squid Game Characters" videos. Its popularity has also led to the creation of app games that put the player in the role of a contestant who is killed if they lose a game.

SCENE RE-ENACTMENTS

Squid Game's pervasive presence on social media has encouraged many content creators to re-enact scenes from the show, which has led to reports of children wanting to also imitate those scenes displayed on social media at home and in school. Much of this content stems from the "Red Light, Green Light" game from the first episode, where contestants attempt to make it past a giant animatronic girl before she shoots them.episode, where contestants attempt to make it past a giant animatronic girl before she shoots them.

Advice for Parents & Carers

USE PARENTAL CONTROLS

Netflix has easily accessible built-in parental controls that allow you to set up a profile for your child with a specific age rating, block them from watching certain shows and even lock their account so it can't be accessed by anyone else. Netflix also allows you to access your child's viewing history to make sure they're not watching anything inappropriate for their age.

CHECK AGE RATINGS

Age ratings on TV shows and films are a way to gauge what is suitable for audiences of different ages. If you are unsure about the content your child is watching, check the age rating to see if the TV show or film is deemed suitable for their age group. If not, try watching the show yourself or talking to other parents who have seen it before to get a better understanding of why it's been rated a certain way.

MONITOR ONLINE ACTIVITY

Squid game has become a social media craze and it's possible your child will see some content related to the show on various platforms. Therefore, it's important to be aware of which websites your child has visited on their smartphone, tablet or laptop, and to also keep an eye out for which accounts they are following on social media platforms, such as Instagram and TikTok.

HAVE OPEN CONVERSATIONS

Making sure your child is comfortable telling you about what they see online can go a long way to ensuring you are kept in the loop about their online use. Showing an interest in what your child is doing online gives you the opportunity to discuss what is and is not appropriate for their age group, and how they might recognise their own feelings towards content they see.

MONITOR BEHAVIOUR

Due to the viral nature of the show, even if your child has not seen Squid Game, it's important to keep an eye on their behaviour. There have been reports from schools of children "playing Squid Game" in the playground and acting aggressively towards the losers as a way to replicate the consequences of losing in the TV show. Viewing content that makes your child feel uncomfortable could also cause them to feel distressed or distracted, so it's important you can easily spot the signs.

WATCH THE SHOW

If you're trying to figure out whether you should let your child watch Squid Game, it might be a good idea to watch the show yourself first. Doing so will allow you to get a better understanding of the show's content and themes, as well as help you decide if this is something you'd feel comfortable with your child being exposed to.

Meet Our Expert

Carly Page is an experienced and highly respected freelance technology journalist, editor and consultant. Previously the editor of tech tabloid The INQUIRER, Carly now works as the news editor for Computer Shopper and IT Pro and writes for a number of publications including Forbes, TechRadar, Tes, The Metro, uSwitch and WIRED.

National Online Safety®
#WakeUpWednesday

Sources: https://www.theguardian.com/tv-and-radio/2021/oct/19/english-council-urges-parents-not-to-allow-children-to-watch-squid-game
https://help.netflix.com/en/node/2064 | https://www.imdb.com/title/tt10919420/parentalguide#advisory-violence

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 app of many 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 WHATSAPP

16+ in UK & EU; 12+ rest of world.

WhatsApp is the world's most popular messaging service, with around two billion users exchanging texts, photos, videos and documents, and making voice and video calls. The app offers end-to-end encryption, meaning messages can only be read by the sender and the recipient(s). Not even WhatsApp can read them. Updates to its privacy policy in 2021 reportedly caused millions of users to leave the app. But the new policy was widely misinterpreted: it only related to WhatsApp's business features, not to personal messages.

'Prize' Scams

WhatsApp users occasionally receive messages from unauthorised third parties or fraudsters pretending to offer prizes – encouraging recipients to click a link to win. A common scam involves a warning that someone's WhatsApp subscription has run out: aiming to dupe them into disclosing payment details. Other scams include instructions to forward a message to earn a gift or reward.

Enabling Fake News

WhatsApp has unfortunately been linked to accelerating the spread of dangerous rumours. In India, some outbreaks of mob violence were reported to have been sparked by false allegations shared on the app. WhatsApp itself took steps to prevent its users circulating hazardous theories and speculation in the early weeks of the Covid-19 pandemic.

Connections with Strangers

To start a WhatsApp chat, you need the mobile number of the person you want to message (they also need to have the app). WhatsApp can also access the address book on someone's device and recognise which of their contacts use WhatsApp. If your child has given their mobile number to somebody they don't know, that person could then use it to get in touch via WhatsApp.

Disappearing Messages

With 'disappearing messages', users can send messages that vanish from WhatsApp after seven days. A new feature also erases photos and videos from chats after they've been viewed. These files can't be saved or forwarded on, making monitoring what children are discussing problematic – and if someone sent your child an inappropriate message, it would be difficult to prove. Content can be reported to WhatsApp, however: ensure your child knows how to do this.

'Only Admins' and Cyberbullying

Group chats and video calls are great for connecting with multiple people in WhatsApp, but there is always the potential for someone's feelings to be hurt by an unkind comment or joke. The 'only admins' feature gives the admin(s) of a group control over who can send messages. They can, for example, block people from posting in a chat, which could make a child feel excluded and upset.

Live Location Sharing

The 'live location' feature lets users share their current whereabouts, allowing friends to see their movements. WhatsApp describes it as a "simple and secure way to let people know where you are." Indeed, it *is* a useful method for a child to let loved ones know they are safe. But if your child is in a chat with people they *don't* know, it means they will be exposing their location to them, too.

Advice for Parents & Carers

Report Potential Scams

Advise your child not to engage with any message that looks suspicious or too good to be true. When your child receives a message from an unknown number for the first time, they will be given the option to report that number as spam. They can also report a contact or a group as spam by tapping on the contact or group name to open their profile and scrolling down to 'report spam'.

Explain about Blocking

If your child receives spam or offensive messages, calls or files from a contact, they should block them. Communication from a blocked contact won't show up on their device and stays undelivered. Blocking someone does not remove them from your child's contact list – they would also need to be deleted from the device's address book. The option to block someone is on their contact info screen.

Create a Safe Profile

Even though someone would need your child's phone number to add them as a contact, as an extra precaution it's worth altering your young one's profile settings to restrict who can see their photo and status. The options are 'everyone', 'my contacts' and 'nobody.' Choosing one of the latter two ensures their profile is protected.

Leave a Group

If your child is part of a group chat that makes them feel uncomfortable, or has been added to a group that they no longer want to be part of, show them how to use the group's settings to leave. If someone exits a group, the admin can add them back in once; if they leave a second time, it is permanent.

Use Location Features Sparingly

If your child needs to use 'live location' to show you or their friends where they are, advise them to share their location only for as long as they need to. WhatsApp gives 'live location' options of 15 minutes, one hour or eight hours. However, your child can manually choose to stop sharing their position at any time.

Delete Accidental Messages

If your child has posted a message in the wrong chat or sent a message that they immediately regret, they can delete it. Tap and hold on the message, choose 'delete' and then 'delete for everyone.' WhatsApp allows seven minutes to delete a message after it's sent – but it's important to remember that recipients may have seen (and taken a screenshot of) a message before it was deleted.

Fact-Check Messages

You can now fact-check messages that have been forwarded at least five times in WhatsApp, by double-tapping the magnifying glass icon to the right of the message. From there, your child can launch a Google search and decide for themselves whether the message was accurate or not. It's a good way to encourage young people to question things they see online.

Meet Our Expert

Parven Kaur is a social media expert and digital media consultant who is passionate about improving digital literacy for parents and children. She has extensive experience in the social media arena and is the founder of Kids N Clicks: a web resource that helps parents and children thrive in a digital world.

National Online Safety®

#WakeUpWednesday

SOURCES: https://www.statista.com/statistics/260819/number-of-monthly-active-whatsapp-users/#:~:text=As%20of%20March%202020%2C%20WhatsApp,US%20dollars%20in%20February%202014, https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/, https://www.whatsapp.com/?lang=en, https://en.wikipedia.org/wiki/Indian_WhatsApp_lynchings, https://www.independent.co.uk/life-style/gadgets-and-tech/news/whatsapp-update-latest-india-hoaxes-forward-messages-app-download-a8498061.html, https://www.bbc.co.uk/news/technology-53441202

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 app of many 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 SNAPCHAT

AGE RESTRICTION 13+

Snapchat is a photo- and video-sharing app which also allows users to chat with friends via text or audio. Users can share images and videos with specific friends, or through a 'story' (documenting the previous 24 hours) visible to their entire friend list. Snapchat usage rose during the pandemic, with many young people utilising it to connect with their peers. The app continues to develop features to engage an even larger audience and emulate current trends, rivalling platforms such as TikTok and Instagram.

CONNECTING WITH STRANGERS

Even if your child only connects on the app with people they know, they may still receive friend requests from strangers. Snapchat's links with apps such as Wink and Hoop have increased this possibility. Accepting a request means that children are then disclosing personal information through the Story, SnapMap and Spotlight features. This could allow predators to gain their trust for sinister purposes.

EXCESSIVE USE

There are many features that are attractive to users and keep them excited about the app. Snap streaks encourage users to send snaps daily, Spotlight Challenges give users to the chance to obtain money and online fame, and the Spotlight feature's scroll of videos makes it easy for children to spend hours watching content.

INAPPROPRIATE CONTENT

Some videos and posts on Snapchat are not suitable for children. The hashtags used to group content are determined by the poster, so an innocent search term could still yield age-inappropriate results. The app's Discover function lets users swipe through snippets of news stories and trending articles that often include adult content. There is currently no way to turn off this feature.

SEXTING

Sexting continues to be a risk associated with Snapchat. The app's 'disappearing messages' feature makes it easy for young people (teens in particular) to share explicit images on impulse. While these pictures *do* disappear – and the sender is notified if it has been screenshotted first – users have found alternative methods to save images, such as taking pictures with a separate device.

DAMAGE TO CONFIDENCE

Snapchat's filters and lenses are a popular way for users to enhance their 'selfie game'. Although many are designed to entertain or amuse, the 'beautify' filters on photos can set unrealistic body image expectations and create feelings of inadequacy. Comparing themselves unfavourably against other Snapchat users could threaten a child's confidence or sense of self-worth.

VISIBLE LOCATION

My Places lets users check in and search for popular spots nearby – such as restaurants, parks or shopping centres – and recommend them to their friends. The potential issue with a young person consistently checking into locations on Snapchat is that it allows other users in their friends list (even people they have only ever met online) to see where they currently are and where they regularly go.

Advice for Parents & Carers

TURN OFF QUICK ADD

The Quick Add function helps people find each other on the app. This function works based on mutual friends or whether someone's number is in your child's contacts list. Explain to your child that this feature could potentially make their profile visible to strangers. We recommend that your child turns off Quick Add, which can be done in the settings (accessed via the cog icon).

CHAT ABOUT CONTENT

Talk to your child about what is and isn't wise to share on Snapchat (e.g. don't post explicit images or videos, or display identifiable details like their school uniform). Remind them that once something is online, the creator loses control over where it might end up – and who with. Additionally, Snapchat's 'Spotlight' feature has a #challenge like TikTok's: it's vital that your child understands the potentially harmful consequences of taking part in these challenges.

CHOOSE GOOD CONNECTIONS

Snapchat has recently announced that it is rolling out a new safety feature: users will receive notifications reminding them of the importance of maintaining connections with people they actually know well, as opposed to strangers. This 'Friend Check Up' encourages users to delete connections with users they rarely communicate with, to maintain their online safety and privacy.

KEEP ACCOUNTS PRIVATE

Profiles are private by default, but children may make them public to gain more followers. Your child can send Snaps directly to friends, but Stories are visible to everyone they have added, unless they change the settings. If they use SnapMaps, their location is visible unless 'Ghost Mode' is enabled (again via settings). It's prudent to emphasise the importance of not adding people they don't know in real life. This is particularly important with the addition of My Places, which allows other Snapchatters to see the places your child regularly visits and checks in: strangers, bullies and groomers could use this information to engage in conversation and arrange to meet in person.

TALK ABOUT SEXTING

It may feel like an awkward conversation (and one that young people can be reluctant to have) but it is important to talk openly and non-judgementally about sexting. Discuss the legal implications of sending, receiving or sharing explicit images, as well as the possible emotional impact. Emphasise that your child should never feel pressured into sexting – and that if they receive unwanted explicit images, they should tell a trusted adult straight away.

BE READY TO BLOCK AND REPORT

If a stranger *does* connect with your child on Snapchat and begins to make them feel uncomfortable through bullying, pressure to send explicit images or by sending explicit images to them, your child can select the three dots on that person's profile and choose report or block. There are options to state why they are reporting that user (annoying or malicious messages, spam, or masquerading as someone else, for example).

Meet Our Expert

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

National Online Safety®
#WakeUpWednesday

Sources: Status of Mind: Social media and young people's mental health | Life in Likes - Children's Commissioner Report | https://support.snapchat.com/en-US https://netsanity.net/snapchat-parent-review/ | IT.com | independent.co.uk, https://mashable.com/article/snapchat-status-snap-maps/?europe=true, eSafety Commissioner, (2017), Young People and Sexting – Attitudes and Behaviours: Research Findings from the United Kingdom, New Zealand and Australia

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 app of many 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 TIKTOK

AGE RESTRICTION 13+

TikTok is a video-sharing social media app which lets people create, view and download looping 15-second clips. Typically, these are videos of users lip-syncing and dancing to popular songs or soundbites (often for comic purposes), enhanced with filters, effects and text. Designed with young people in mind, TikTok skyrocketed in popularity in 2019 and has featured near the top of download charts ever since. It now has around a billion users worldwide.

AGE-INAPPROPRIATE CONTENT

Most videos appearing on a child's feed are light-hearted and amusing. However, some clips have been reported for featuring drug and alcohol abuse, themes of suicide and self-harm, or young teens acting in a sexually suggestive way. The sheer volume of uploads is impossible to moderate entirely – and since TikTok Jump's introduction in mid-2021, users can view third-party content outside the app.

18 CENSORED

EXPLICIT SONGS

W&#*!

TikTok primarily revolves around videos of users lip-syncing and dancing to music. Inevitably, some featured songs will contain explicit or suggestive lyrics. Given the app's young user-base, there is a risk that children may view older users' videos and then be inclined to imitate any explicit language or suggestive actions.

TIKTOK FAME

The app has created its own celebrities: Charli D'Amelio and Lil Nas X, for example, were catapulted to fame by exposure on TikTok – leading to many more teens attempting to go viral and become "TikTok famous". While most aspiring stars hoping to be 'the next big thing' will find it difficult, setbacks may in turn prompt them to go to even more drastic lengths to get noticed.

HAZARDOUS VISIBILITY

Connecting with others is simple on TikTok – including commenting on and reacting to users' videos, following their profile and downloading their content. The majority of these interactions are harmless, but – because of its abundance of teen users – TikTok *has* experienced problems with predators contacting young people.

ADDICTIVE NATURE

Like all social media, TikTok is designed to be addictive. It can be hugely entertaining – but that also makes it hard to put down. As well as the punchy nature of the short video format, the app's ability to keep users intrigued about what's coming next mean it's easy for a 5-minute visit to turn into a 45-minute stay.

IN-APP SPENDING

There's an in-app option to purchase 'TikTok coins', which are then converted into digital rewards for sending to content creators that a user likes. Prices range from 99p to an eye-watering £99 bundle. TikTok is also connected with Shopify, which allows users to buy products through the app.

Advice for Parents & Carers

TALK ABOUT ONLINE CONTENT

Assuming your child is above TikTok's age limit, talk to them about what they've viewed on the app. Ask their opinion on what's appropriate and what isn't. Explain why they shouldn't give out personal details or upload videos which reveal information like their school or home address. In the long run, teaching them to think critically about what they see on TikTok could help them to become social-media savvy.

MAINTAIN PRIVACY SETTINGS

The default setting for all under 16s' accounts to 'private'. Keeping it that way is the safest solution: it means only users who your child approves can watch their videos. The 'Stitch' (which lets users splice clips from other people's videos into their own) and 'Duet' (where you build on another user's content by recording your own video alongside their original) features are now only available to over 16s. This might clash with your child's ambitions of social media stardom, but it will fortify their account against predators.

LEARN ABOUT REPORTING AND BLOCKING

With the correct privacy settings applied, TikTok is a relatively safe space. However, in case something *does* slip through, make sure your child knows how to recognise and report inappropriate content and get them to come to you about anything upsetting that they've seen. TikTok allows users to report anyone breaching its guidelines, while you can also block individual users through their profile.

ENABLE FAMILY PAIRING

'Family Pairing' lets parents and carers link their own TikTok account to their child's. Through your mobile, you can control your child's safety settings remotely – including limiting screen time, managing their ability to exchange messages (and with whom) and blocking a lot of age-inappropriate content. TikTok's Safety Centre also provides resources for parents and carers to support online safety among families. These resources can be found on their website.

USE RESTRICTED MODE

In the app's 'Digital Wellbeing' section, you can filter out inappropriate content (specific content creators or hashtags, for instance) using 'Restricted Mode'. This can then be locked with a PIN. You should note, though, that the algorithm moderating content isn't totally dependable – so it's wise to stay aware of what your child is watching.

MODERATE SCREEN TIME

As entertaining as TikTok is, you can help your child to manage their time on it in the 'Digital Wellbeing' section. Under 'Screen Time Management', you can limit the daily permitted time on the app (in increments ranging from 40 minutes to two hours). This preference can also be locked behind a PIN. That way, your child can get their regular dose of TikTok without wasting the whole day.

Meet Our Expert

Parven Kaur is a social media expert and digital media consultant who is passionate about improving digital literacy for parents and children. She has extensive experience in the social media arena and is the founder of Kids N Clicks: a web resource that helps parents and children thrive in a digital world.

SOURCES TikTok.cpm

National Online Safety®

#WakeUpWednesday

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

Facebook is an online social media platform that has over 2 billion users across the globe. It was initially for university students but soon expanded out and since 2006, anyone over the age of 13 is able to join the platform. It is available on all devices from your desktop and laptop computer to smartphones and tablets. Users can add photos and videos, update their status, interact with others and catch up with the latest news. Despite requiring users to be over 13, there are no age verification measures and children can easily create an account. It's therefore important that parents familiarise themselves with the main features of the platform to ensure their young ones remain safe if and when they use it.

AGE RESTRICTION 13+ If under 18, supervision of a parent or legal guardian required.

What parents need to know about FACEBOOK

ADDICTIVE NATURE

Facebook can be hugely addictive as it offers a physiological high and a quick reward cycle which comes from the likes and comments on shared posts. Communication is so instant now that teenagers are always checking, and it can sometimes feel like self-worth. This keeps children going back, encouraging them to post things and also increases the Fear Of Missing Out (FOMO) that is commonplace today. On the flip side, because of the way teenagers interact these days through Facebook and Facebook Messenger, they can seem addicted even when they're not.

CYBERBULLYING

Around a quarter of children have experienced online abuse, according to Ofcoms 2019 'Online Nation' report. Figures show that 23% have been cyberbullied, 39% subjected to abusive language and a fifth have been trolled. On Facebook, teenagers can receive communication in a number of ways, from private messages in Messenger to public comments on profiles, pages and posts to pages or groups set up just to torment a victim. Exclusion from pages or groups to cause the victim to feel left out has also been seen.

FUTURE IMPACT

Regardless of age, anything that's posted on Facebook, or other social media platforms, develops a personal brand and leaves a digital footprint that is there forever. It can be difficult to explain the consequences but many universities (and employers) look at Facebook before making a decision on accepting people. It is therefore wise to always think twice before posting anything online you wouldn't want people to hear or see offline.

STRANGERS/FAKE PROFILES

Generally, people are who they say they are online. That said, much like the real world, Facebook isn't free of malicious users and children have received friend requests from people they don't know, including individuals who may look to take advantage of young and impressionable children.

OVERSHARING

Facebook encourages you to share "what's on your mind" but children need to be aware of what they're revealing about themselves online. Facebook allows users to share their location, create live videos and much more. Some photos can be traced using file data, too, so it's important to keep a tight group and share only with people you know.

INAPPROPRIATE ADS

While Facebook is getting ever stricter on the content of ads and who they are targeted to, there is still the chance that children could be subject to ads during their experience on the platform. This could be innocuous but is worth bearing in mind when using the app.

LIVE STREAMING

Facebook Live provides users with the ability to stream video live-time to their friends and followers or watch other people's broadcasts live. During the video, people can react and comment and it's difficult to moderate the content given everything happens in real-time. This could mean your child is exposed to inappropriate material or worse still, could be cajoled into doing something online by others which they wouldn't normally do.

PRIVATE MESSAGING

Facebook Messenger is closely linked to your Facebook profile and provides the ability to share private messages away from friends and family. It is therefore important that parents ask their children who they are communicating with and ensure that the only people they are exchanging messages with are people that they also know in real life.

National Online Safety® #WakeUpWednesday

Safety Tips For Parents

MAKE PROFILES PRIVATE

Within the settings of a Facebook account, you can choose whether a profile is public or private. Make sure that your child's setting is switched to private. This way they will only be able to interact with friends and people they know within the platform.

LEAD BY EXAMPLE

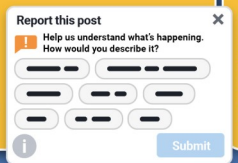
Show your children how and why you use Facebook. This will help to demonstrate that it can be used safely when used in an appropriate manner and help to reduce the risk of them encountering harmful content.

SHARE DEVICES

Depending on the age of your children, it's worth considering letting them use Facebook from a general family iPad or laptop. This allows them to use it without being constantly connected everywhere they go and may give you more reassurance around what they are doing on the app.

REPORT VIOLATIONS

On Facebook you're able to hide people or groups and report things that are harmful. Make sure you spend some time to show your children how this works and why it's important to do so before they start spending serious time on the platform.



RESPECT BOUNDARIES

As with anything, there are potential risks and dangers on Facebook but once you've talked about the ideas of safety on the platform, give children some space. Trust them to make smart choices but always be open to talking about social media.

CHECK-IN

Once they've had some time to use the platform, don't be afraid to check in and see if there's anything on Facebook they'd like to discuss. This isn't always easy but being open with your children is the best way to deal with any issues head on.

Meet our expert

Alex Wright is a former Facebook employee and social media expert with over 15 years' experience working in digital media. He has worked with some of the biggest organisations in the world and has a wealth of knowledge in understanding how social media platforms work and how they engage their audience.

SOURCES: http://facebook.com, https://www.independent.co.uk/life-style/social-media-addiction-young-children-under-five-youtube-instagram-a8953411.html, https://www.independent.co.uk/life-style/health-and-families/cyberbullying-social-media-children-online-abuse-facebook-research-ofcom-ico-a8936366.html, https://thriveglobal.com/stories/how-social-media-affects-our-ability-to-communicate/, https://www.care.com/c/en-gb/stories/4275/5-dangers-of-social-media-to-discuss-with-you/

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

What parents need to know about INSTAGRAM

AGE RESTRICTION 13+ Anyone over the age of 13 can create an account

Instagram is a hugely popular social networking app with over 1 billion users worldwide. The app, which is accessible on iOS and Android devices, allows users to upload images and videos to their feed, create interactive 'stories', exchange private messages or search, explore and follow other accounts they like. Images and videos can be transformed with an array of filters to edit the shot before sharing and anyone with an account can see others' online 'galleries' if their account is not private. To make posts easier to find, users can include searchable hashtags and captions to their uploads. That's why we've created this guide to help parents and carers understand exactly what Instagram is about.

HOOKED ON SCROLLING

Many social media platforms, Instagram included, have been designed in a way to keep us engaged on them for as long as possible. Behavioural economist, Nir Eyal, calls this the 'Hook Model' and the Instagram feed is a great example of this. Children and adults may find themselves scrolling to try and get a 'dopamine release'. Scrolling may become addictive and it can be difficult to stop until children find that 'something' they are looking for, quickly losing track of time as they get deeper into their Instagram feed.

SLIDING INTO DMS

Direct messages (or DMs) on Instagram allow users to share posts, images, videos, voice messages and calls between each other privately (or in a private group). Even if your child's account is set to private, anybody has the option to message them and send them content. If the person is not on your child's friends list, the message will still be sent to their inbox but the user has to accept their request to see the message.

INFLUENCER CULTURE

Influencers are sometimes paid thousands of pounds to promote a product, service, app and much more on social media. When celebrities or influencers post such an advert, they should add a disclaimer somewhere in the post which states that they have been paid for it. Commonly, this is well-hidden in the hashtags or in the comments of their post, making it unclear that their photo/video is actually an advert. This can be very misleading to young people who may be influenced into buying/wanting something promoted by somebody they admire, creating a false sense of reality and potentially affecting their mental health and wellbeing.

IMPACT ON WELLBEING

In a report by the RSPH, Instagram was ranked the worst for young people's mental health. Using filters on photos on Instagram can set unrealistic expectations and create feelings of inadequacy. Children may strive for more 'likes' by using realistically edited photos. Judging themselves against other users on the app might threaten their confidence or self-worth. In early 2019, Instagram banned images of self-harm and suicide, following the suicide of 14-year-old Molly Russell, who had reportedly been looking at such material on the platform. They since extended the ban to include drawings, cartoons and memes.

LIVE STREAMING TO STRANGERS

Live streaming on Instagram allows users to connect with friends and followers in real-time and comment on videos during broadcast. If your child's account is private, only their approved followers can see their story. It's important to note they may have accepted a friend request from someone they don't know, which means they could be live streaming to strangers. Children also risk sharing content they later regret, which could be re-shared online for years to come. Public accounts allow anybody to view, so we suggest your child blocks followers they don't know. In early 2019, data gathered by the NSPCC found that sex offenders were grooming children on Instagram more than on any other online platform.

IN-APP PAYMENTS

Instagram allows payments for products directly through the app. It operates under the same rules as Facebook Payments, which state that if you are under the age of 18, you can only use this feature with the involvement of a parent or guardian.

EXPOSING LOCATION

Public locations can be added to a user's photos/videos and also to their stories. While this may seem like a good idea at the time, it can expose the location of your child. This is particularly more of a risk if it is on their story, as it is real time. A photo which includes landmarks in the area, their school uniform, street name, house and even tagging in the location of the photo uploaded to Instagram can expose the child's location, making it easy to locate them. If their account is public, anyone can access their account and see their location.

HIJACKED HASHTAGS

Hashtags are an integral part of how Instagram works, but they can come with risks. One person may use a seemingly innocent hashtag with one particular thing in mind, and before you know it hundreds of people could be using the same hashtag for something inappropriate or dangerous that your child shouldn't be exposed to.

IGTV

Instagram TV (IGTV) works similar to YouTube. Users can watch videos from favourite accounts on the platform or create their own channel and post their own videos. It's important to note anyone can create an Instagram TV channel and doesn't have to be friends with a person to follow an account and watch their videos. In 2018 Instagram apologised and removed some of its TV content which featured sexually suggestive imagery of children. As the feature may encourage spending more time using the app, it's important to set time limits to avoid children's sleep or education being disturbed.

Top Tips for Parents & Carers

RESTRICT DIRECT MESSAGES

If your child receives a message from somebody they do not know, encourage them not to accept their message request and 'block' this person; this is the only way to stop them messaging your child again. Children can also 'tap and hold' the individual message to report it directly to Instagram as well as reporting the account itself.

LOOK OUT FOR #ADS

In 2019, the UK's Competition and Markets Authority launched an investigation into celebrities who were posting adverts on social media and not declaring that they were paid for. Influencers must clearly state that they have been paid for their posts, for example using a hashtag like #ad or #sponsored. Teach your child to look out for the signs of a paid post/advert and discuss with them that not everything they see from celebrities is their personal choice and opinion.

MANAGE NEGATIVE INTERACTIONS

If your child is receiving unwanted or negative comments, they can block that account so that they can't interact with them. This stops them seeing and commenting on their posts, stories and live broadcasts. In addition, your child can instantly delete unwanted comments from their posts, turn them off completely and control who can tag and mention them in comments, captions or stories, from everyone, only people they follow, or no one at all.

MANAGE DIGITAL WELLBEING

Instagram now has an in-built activity dashboard that allows users to monitor and control how much time they spend on the app. Users can add a 'daily reminder' to set a limit on how much time they want to spend on Instagram, prompting them to consider if its been too long. In addition, once users have caught up with all the previous posts since they last logged on, they'll receive a 'You've completely caught up' message. Both features can help you have a conversation with your child about how much time they are spending on the app and to set healthy time limits.

PROTECT PERSONAL INFORMATION

Your child may unknowingly give away personal information on their profile or in their live streams. Talk to them about what their personal information is and make sure that they do not disclose anything, including their location, to anyone during a livestream, comment, direct message or any other tool for communication on the platform, even to their friends.

USE A PRIVATE ACCOUNT

By default, any image or video your child uploads to Instagram is visible to anyone. A private account means that you have to approve a request if somebody wants to follow you and only people you approve will see your posts and videos. Children should also use a secure password and enable a two-factor authentication to add an extra layer of security to their account.

FILTER INAPPROPRIATE COMMENTS

Instagram has an 'anti-bullying' filter, which hides comments relating to a person's appearance or character, as well as threats to a person's wellbeing or health. The filter will also alert Instagram to repeated problems so that they can take action against the user if necessary. This is an automatic filter, which should always be enabled. Children can also report abusive behaviour or inappropriate/offensive material directly to Instagram from the app. This includes posts, comments and accounts.

TURN OFF SHARING

Even though this feature will not stop people from taking screenshots, it will stop others being able to directly share photos and videos from a story as a message to another user. This feature can be turned off in the settings. We also recommend turning off the feature which automatically shares photos and videos from a story to a Facebook account.

REMOVE PAYMENT METHODS

If you are happy for your child to have a card associated with their Instagram account, we suggest adding a PIN which needs to be entered before making a payment; this will also help prevent unauthorised purchases. This can be added in the payment settings tab.

DON'T FORGET TO BE VIGILANT & TALK TO YOUR CHILD ABOUT THEIR ONLINE ACTIVITIES!

Meet our expert

Parven Kaur is a social media expert and digital media consultant who is passionate about improving digital literacy for parents and children. She has extensive experience of working in the social media arena and is the founder of Kids N Clicks, a web resource helping parents and children thrive in a digital world.

NEW FOR 2020 INSTAGRAM REELS

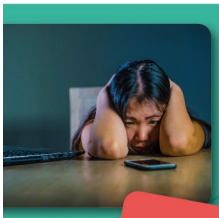
Instagram Reels is the latest update from Instagram that gives users the ability to record and edit 15-second multi-clip videos with audio, effects, and new creative tools. It is the apps answer to TikTok and can be accessed via the Stories feature. Reels can be shared with friends and family, however, if your child has a public account, it could be shared wider via 'Explore' and viewed by millions of strangers online.

National Online Safety®

#WakeUpWednesday

SOURCES:
https://about.instagram.com/about-us | https://about.instagram.com/community/safety | https://www.bbc.co.uk/news/uk-47410520

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



The Diana Award definition of bullying is "repeated negative behaviour that is intended to make others feel upset, uncomfortable or unsafe." Cyberbullying is bullying which takes place online. It can involve anything from sending messages to posting offensive comments to uploading and sharing private or embarrassing photos. It is classed as an indirect form of bullying when compared to verbal or physical bullying, given it usually takes place through a digital device. However, for those experiencing bullying behaviour, the consequences can be just as serious and have far reaching effects.

What schools need to know about CYBERBULLYING

3 KEY ASPECTS OF BULLYING BEHAVIOUR

There are three key aspects of bullying behaviour, namely that it is repetitive, negative and intentional. These behaviours apply both offline and online. Cyberbullying can almost heighten these behaviours, particularly with access to the internet available 24/7 and the different ways in which those displaying bullying behaviour online can target others. The fact that they can also easily hide their identity online can make cyberbullying much more difficult to stop.

DIFFERENT DEVICES & CHANNELS

Cyberbullying can take place over any device connected to the internet which allows for two-way communication. This includes mobile phones, tablets, computers and even games consoles as it becomes more and more common for players to chat to other players whilst playing online. From a snapshot of 1,400 students surveyed by the Diana Award in 2018, 33% of young people admitted to have experienced bullying on social media, 11% via text message and 12% whilst online gaming.

WHAT LEADS TO CYBERBULLYING

There is never any justification for cyberbullying and those who display bullying behaviour need to be held to account for their actions. Nonetheless, it can useful to try and understand some of the factors that may lead young people into bullying behaviour. For example, family issues, personal difficulties and a lack of positive reinforcement may push some young children into bullying others as a form of coping mechanism. Similarly, those exhibiting bullying behaviour may blame their targets for provoking their behaviour in the first place or engage in bullying behaviour as a call for attention if they lack social skills or understanding. Others may view their position as dominant which makes themselves less vulnerable to being bullied or they replicate behaviour they have experienced themselves in the past.

SIGNS AND SYMPTOMS

Cyberbullying can affect anyone, at any time, at any place. The impacts of cyberbullying can be long-lasting and leave people feeling scared, anxious and lonely. Some of the more obvious signs that those experiencing bullying behaviour might show include weight loss, crying, mood changes, depression and regularly avoiding school. Other symptoms, which might be less obvious to spot and would be difficult to pick up on in isolation, may include changes in body language like hunched shoulders, walking slower or an inability to make eye-contact. In extreme cases, those experiencing bullying behaviour may have unexplained marks or scars which could be evidence of self-harm.

National Online Safety®

#WakeUpWednesday

Tips for School Staff

TAKE A WHOLE SCHOOL APPROACH

In taking a whole approach towards cyberbullying, schools can cultivate a culture that relies on positivity and behaviour that is emulated by ALL members of the school community including staff, support staff, senior leaders, governors and parents and carers.

BUILD CONFIDENCE IN DEALING WITH INCIDENTS

This can be achieved by having clear knowledge of what constitutes bullying behaviour, having clear sanctions and courses of action and continually updating your knowledge of safety procedures regarding online and offline incidents.

USE CHILDREN AND YOUNG PEOPLE AS A RESOURCE

Ensure you understand what is influencing the behaviour of young people in your community. If schools know what their students are engaging with, it can be easier to develop and implement relevant and effective tactics / strategies to counter cyberbullying issues.

UNDERSTAND THE CAUSES OF BULLYING

As previously mentioned, sometimes those who are behind the bullying are in need of support just as much as those who being targeted. In better understanding the cause of the issue, schools can better position themselves to tackle the problem and also adequately support both those displaying and experiencing the bullying behaviour. Taking a proactive approach means that schools can gear themselves to tackle issues specific to their school environment, rather than treating each case the same.

ENSURE ALL STAFF KNOW THEIR ROLES AND RESPONSIBILITIES

All staff have a role to play in educating and supporting children who are affected by cyberbullying, not just those responsible for safeguarding or online safety. Regular training, continuous professional development and clear school policies can help to empower staff in effectively managing any cyberbullying issues and in providing a united staff front on zero tolerance to all bullying behaviour.

Ask For Help

For further support, advice or guidance to support you students at school, or to sign up to our FREE Anti-Bullying Ambassadors training events, head to www.antibullyingpro.com

www.nationalonlinesafety.com Twitter - @natonlinesafety Facebook - /NationalOnlineSafety

What Parents & Carers Need to Know about FREE SPEECH VS HATE SPEECH

Everyone has the right of 'freedom of expression.' This is the right to voice your opinions and share information and ideas with others. It is not the right to say whatever you want. We all have a responsibility to use freedom of expression properly by not saying things that are grossly offensive or threatening, or encouraging hateful activity, thereby undermining the rights of others. Both online and offline, hate speech targets those who are different to the speaker in some way. Communication attacking or discriminating against groups and individuals (because of characteristics like race or religion) is hate speech, not free speech.

What is Free Speech?

Free speech is the principle that an individual is allowed to share information, opinions and ideas without fear of retaliation, censorship, or legal consequences. Here's why free speech is important ...

The Human Rights Act states that everyone has the right to express themselves freely and hold their own opinions – even if those views are unpopular and could offend others.

Freedom of expression encourages listening to others and allowing opposing views to be heard. It's important that we respect someone's opinion, even if we disagree with it.

Any idea could potentially offend someone: Both Galileo and Darwin's theories, for example, were originally incredibly offensive to many. Freely exchanging ideas promotes progress.

The ability to challenge others' views – and have ours challenged, too – is healthy, as it helps us learn to deal with criticism and to think seriously about what we say and believe.

It's a powerful way to push for change. Many modern rights – such as women being allowed to vote, or decent working conditions – couldn't have been achieved without free speech.

Freedom of expression also includes the right not to do something: such as not standing up or singing for the national anthem, even though some people would deem that offensive.

What is Hate Speech?

Hate speech is any communication which displays prejudice against someone's identity. It can be derogatory, demonising and dehumanising statements, threats, identity-based insults, offensive name-calling and slurs. Some common types of hate speech include ...

Targeting people or groups because of their race, gender or gender identity, sexuality, nationality, religion or a disability.

Content which dehumanises individuals or groups based on those attributes, such as referring negatively to them as animals, inanimate objects or other non-human entities.

Calling for violence or hatred against certain people or groups, and justifying and glorifying these actions.

Claiming that specific types of people are physically, mentally or morally inferior, or even that they are criminals.

Promoting the exclusion or segregation of certain groups of people, or discrimination against them, because of who they are (e.g. their race or gender).

Making up or repeating insults about a person or group because something about their identity (for example, religious beliefs or a disability) is different to the person who's posting.

For further information and reporting:

Amnesty International:
https://www.amnesty.org/en/what-we-do/freedom-of-expression/

True Vision:
https://www.report-it.org.uk/reporting_internet_hate_crime

Report Harmful Content:
https://reportharmfulcontent.com/?lang=en

STOP HATE UK
STOP HATE. START HERE

National Online Safety®
#WakeUpWednesday

At National Online Safety we believe in empowering parents, carers and educators with the information they need to hold an informed conversation about online safety with their children, should they feel it is needed. Please visit nationalonlinesafety.com for further guides, hints and tips for adults.

Part of our Social Media & Live Streaming Series

NOS Social Media & Live Streaming

Brought to you by National Online Safety®

www.nationalonlinesafety.com

What you need to know about... VIDEO STREAMING APPS & SITES

What are they?

'Video Streaming Apps & Sites'

Video streaming apps and sites can allow people to share activities and hobbies with others in real time or watch their favourite films and TV shows online. There are different types of video streaming services. Twitch is used for watching others play video games in real time; you can watch YouTube live and watch Netflix, Amazon Prime or Apple TV with friends and family. Video streaming has gained popularity in the last few years because there is a sense of community when watching with others and people can comment on videos and ask questions in real-time.

Know the Risks

Inappropriate videos

When watching on video streaming apps, it is difficult to filter the content that is out there. For instance, when a child is watching a YouTube video, they will get recommendations for other similar videos. The risk is even higher with videos which are live, as children could be watching inappropriate content in real time.

Chatting with strangers

Video streaming apps or sites increase the risk of children communicating with strangers online. For example, most YouTube videos allow users to comment on the video. Whilst children could be watching something innocent, the comments section can be used by groomers to try and direct them towards private messaging.

Binge-watching

Children can easily fall into 'binge-watching' on video streaming apps which can impact on sleep, mood and their ability to concentrate on other things. The autoplay function can make it difficult to find time for a break and often the recommended content is similar to what children are already watching based on the algorithms used.

Screen addiction

In addition to binge-watching, most video streaming apps are available across all devices with an internet connection which can mean increased screen time. Popular apps, such as Netflix and Amazon Prime, have huge libraries of content which can mean hours of viewing time and potentially less time spent on learning, playing outside or interaction with friends and family.

Safety Tips

Check age-ratings

13+

Ensure that children are at the right age to use the app. Most video streaming apps require users to be at least 13 years old. Be clear on what apps and sites children can use. Encourage them to never participate in online discussions that are offensive and never interact with strangers or people they don't trust.

Change privacy settings

Check the privacy setting of children's app. Ensure that for whichever app they are using, the settings are set to private and disable comments if applicable. Furthermore, set screen time restrictions via the app or the device to limit children's use.

Implement parental controls

Activate parental controls your child's devices and apps. This will prevent them from accessing content they shouldn't. For instance, on Netflix, create a kids profile. This way they will only be able to view videos appropriate for their age group. Likewise, use YouTube Kids over YouTube or apply restrictions and turn off features such as autoplay.

Spend time on the app

Before allowing children to access a video streaming app, spend some time browsing through its content. Familiarise yourself with how it works, what content is available and what your child wants to watch. Check-in regularly and ask what they enjoy watching and how it makes them feel.

Action & Support

Report inappropriate content

If a child comes across inappropriate content or something that makes them feel uncomfortable on an app such as YouTube, you can report the content and the person who has uploaded the content to the platform. If a stranger is looking to engage with your child, block them and report them.

Have an open and honest conversation

Adults can review the TV shows and films that have been watched many video streaming apps. If a child seems upset or shocked by something they have seen or if you are concerned about anything they've viewed, try to talk to them about it and have an open and honest conversation to help understand any concerns.

Encourage other activities

If you think a child is spending too much time on a video streaming app, try to foster their interest in other activities or hobbies away from their device. Encourage them to get outdoors, play with friends, play board games or just simply spend more time together with you.

Our Expert

Parven Kaur

Parven Kaur is social media expert and digital media consultant who is passionate about improving digital literacy for parents and children. She has extensive experience in the social media arena and is the founder of Kids N Clicks; a web resource that helps parents and children thrive in a digital world.

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 platform of many 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 NETFLIX

Netflix is a subscription-based streaming service that allows users to watch TV shows and movies on any internet-enabled device that supports the software, such as smart TVs, phones and tablets. The pandemic saw a surge in children consuming on-demand content as many families relaxed their screen-time rules. Netflix's diverse range of programming caters for all age groups – so it's important for parents to recognise the potential risks of children using the service and the measures to help their child enjoy a safe streaming experience.

INAPPROPRIATE CONTENT

Netflix produces and curates an extensive catalogue of content that can provide hours of entertainment. If they share the same user account as an adult, this can potentially lead to children accidentally viewing all manner of inappropriate content, including nudity, profanity and extreme violence. This can happen easily on shared accounts, as Netflix cannot establish who's watching.

BINGE-WATCHING

Netflix allows users to view shows and movies quickly and easily without adverts or interruptions, making excessive screen time a concern. Binge-watching has become more common during the pandemic, due to Netflix's regularly updated content and algorithms which recommend content very similar to what's previously been enjoyed. Marathon viewing sessions can lead to children staying up too late, affecting their mood and concentration the next day.

SCREEN ADDICTION

From TVs and phones to consoles and tablets, Netflix is available on almost any device with an internet connection – making it extremely difficult to manage children's screen time. The service is now adding games to its mobile app, tempting users to spend even more time on the platform. Screen addiction can distract children from important activities like schoolwork and socialising, and can impact their health by reducing their exercise and sleep.

HACKING ATTEMPTS

With millions of users worldwide, Netflix is often targeted by hackers who try to steal usernames and passwords to gain access to people's accounts. If successful, they can then steal payment details or try to sell stolen personal data on the dark web, providing other criminals with a profitable opportunity. Netflix also doesn't provide two-factor authentication, making the hackers' task that little bit easier.

CONTACT FROM STRANGERS

Netflix's Teleparty feature became popular during lockdown periods as it allows users from different households (friends and relatives, for example) to synchronise when they watch content. It requires an access link to be sent to the people you wish to invite: the link, however, can also be distributed to people you *don't* know. A text chat feature enables interaction with the other users in real-time: this represents a risk to children if a stranger gains access to the Teleparty.

Advice for Parents & Carers

KEEP ACCOUNTS SECURE

Netflix doesn't use two-factor authentication, so a strong password is vital. Your child's Netflix password should be unique (not one they've used elsewhere) and a minimum of eight characters with a mix of letters, numbers and symbols. Emphasise not to share their login details with anyone and remind them to always log out after using the app – so their account remains inaccessible, even if their device is lost or stolen.

CHECK MATURITY RATING

Netflix warns about content that includes violence, sex, profanity and nudity. These warnings form part of the show or movie's 'maturity rating'. Users can restrict age ratings to avoid children viewing age-inappropriate content. On their profile, open the Profile and Parental Control settings and choose the maturity level for the shows and movies you want to allow.

CREATE A KIDS' PROFILE

Setting up a Netflix Kids experience profile means your child can only access content which is suitable for children aged up to 12 years. All other content is automatically blocked. This rating can be further restricted via the child's profile settings. Setting up a Netflix Kids experience profile will help to prevent your child from viewing age-inappropriate content.

SET UP PROFILE PINS

Netflix account holders can lock profiles using a four-digit PIN. Doing this can prevent your child from accessing the wrong account and viewing content that isn't appropriate for their age. Try setting a PIN for each account on your Netflix app – ideally avoiding numbers that would be easily guessed, such as dates of birth. Remember not to share these PINs with anyone, including family.

SWITCH OFF AUTO-PLAY

When a show or movie concludes, Netflix's algorithms select content with similar themes that it thinks your child will enjoy next. This new content starts automatically after a 10-second countdown. Disabling this auto-play feature reduces the possibility of your child being shown something inappropriate and provides a natural break to help prevent them becoming too immersed in Netflix.

CHECK VIEWING HABITS

Netflix has tools which enable parents and carers to monitor what their child has been watching. Selecting 'Viewing Activity' in each profile's account settings displays a list of what content has been viewed (and when). This can reassure parents that their child is watching age-appropriate content and can open avenues for discussing your child's favourite shows and movies, and why they like them.

Meet Our Expert

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

National Online Safety®

#WakeUpWednesday

Sources: www.help.netflix.com | www.about.netflix.com | www.ofcom.org.uk

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 issue of many which we believe trusted adults should be aware of. Please visit www.nationalonlinesafety.com for further guides, hints and tips for adults.

What Parents and Carers Need to Know about SOCIAL BOTS

WHAT ARE SOCIAL BOTS?

Bots are computer-generated accounts which sit on social media, masquerading as humans. While many are harmless or even have good intentions, others are designed to extort, sell products, spread propaganda or bully human users. Bots – short for 'robots', of course – are often confused with state-funded troll accounts; the two can be difficult to tell apart. However, if the results are the same, then both should be treated similarly.

KNOWING THE RISKS ...

ASTROTURFING

Propaganda and conspiracy theories are usually niche interests on social media. But with an army of thousands of bots amplifying posts through retweets and shares, people can make their messages travel further and appear to reflect mainstream opinion. Known as 'astroturfing', this can make children more susceptible to questionable beliefs.

CYBERBULLYING

Bots can be set to hunt for certain search terms or opinions and then automatically reply aggressively to anybody who uses them in a message. This means that if your child posts something that whoever programmed the bot doesn't like, they may be deluged with angry messages from fake accounts – which can be overwhelming and comparable to cyberbullying.

EXTORTION

Criminals use bots to trap users into sextortion or online blackmail scams. The bot cultivates a flirtatious online relationship with the victim, then persuades them into a video chat during which they are tricked into posing inappropriately or carrying out a sexual act. This footage is recorded, and threats are then made to release it to the victim's friends and family unless money is paid.

SHADY SELLING

Bots are often used for illicit advertising – that is, they spam social media platforms with links to commercial websites. Additionally, some unscrupulous influencers have been found to use bots to artificially inflate their number of followers and the engagement with their account – making them seem more popular and therefore able to charge companies more to work with them.

SPOTTING THE SIGNS ...

BEWARE PROLIFIC POSTING

Bots post a superhuman amount of content. A visit to their profile usually proves they're responding to people far faster than a human could. Check their join date and number of followers. If the account has been around for ages and still doesn't have any friends, it probably isn't a real person. A brand-new page is also a red flag.

NOTICE ODD USERNAMES

Finding a social media username that isn't taken can be difficult. People often end up with their name and some numbers – but not the way bots do it. A username like johnsmith5273 is either a sign of a random number generator or a site offering an unwieldy alternative because the preferred name is taken, which isn't something most humans would accept.

VERIFY PROFILE PICS

Check a user's authenticity by investigating their profile picture: bots obviously don't have faces, so they tend to skim publicly available photos to try to fool people. Put suspicious pics through a reverse-image search like TinEye – you might find they actually belong to someone else or are stock images.

CHECK THE CONTENT

Bots can't think for themselves and usually just exist to amplify somebody else's message. Try copying and pasting the text into the search function on Twitter, for example, and see if it's being said anywhere else. If a lot of similar-looking accounts are saying the same thing, you're probably looking at a bot army.

Advice for Parents & Carers

SPOT THE BOTS

Forewarned is forearmed, so if your children aren't that familiar with the world of bots yet, explain what to look for using the tips in this guide. At the moment, most bots still aren't that sophisticated – so finding accounts which are designed purely to troll people or spread misinformation isn't hugely difficult, even for an untrained eye.

BLOCK AND MOVE ON

Your child isn't obliged to be friends with anyone online, bot or not. Pretty much every social media app has a block button, and you should encourage your child to use it whenever something or someone is making their digital lives less than pleasant. If everyone blocked malicious bots rather than engaging them, they wouldn't pose a problem.

BE SUSPICIOUS

While many people have made lifelong friends over the internet, it's important not to be too trusting. Random strangers adding you on Facebook could well be bots, so do some background checks: do they have any mutual friends? Is it a new account? Even if everything seems fine, encourage your child to be cautious: warn them of potential risks.

Meet Our Expert

Alan Martin is an experienced technology journalist and the former deputy editor of technology and internet culture website Alphr. Now freelance, he has contributed articles to publications including the *New Statesman*, CNET, the *Evening Standard*, *Wired*, *Rock Paper Shotgun*, *Gizmodo*, *Pocket Gamer*, *Stuff*, *T3*, *PC Pro*, *Macworld*, TechRadar and Trusted Reviews.

National Online Safety®

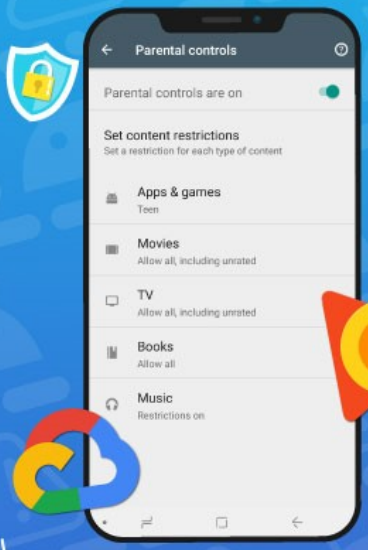
#WakeUpWednesday

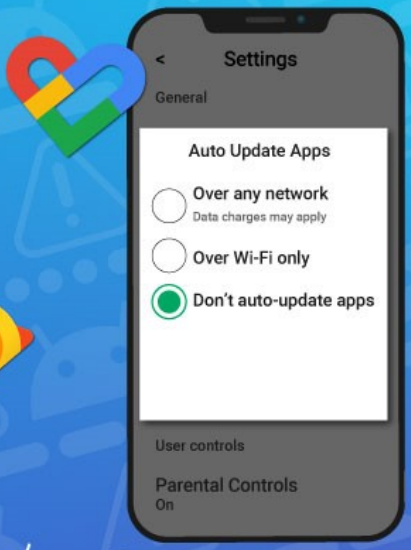
SOURCES: https://www.computing.co.uk/feature/3085226/the-positive-case-for-twitter-bots | https://www.nytimes.com/2018/02/18/world/europe/russia-troll-factory.html
https://truepublica.org.uk/united-kingdom/propaganda-automated-bots-defending-the-government/ | https://www.bbc.co.uk/radio/presenters/james-obrien/what-are-the-twitter-users-with-eight-numbers/

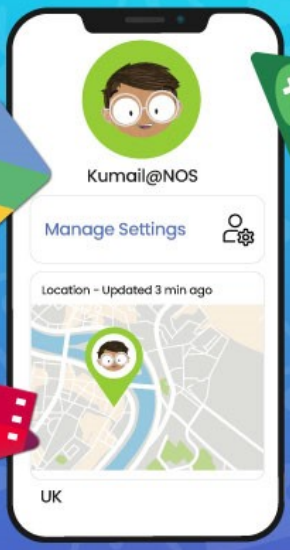
How to Set up PARENTAL CONTROLS for APPS

Android Phone

On Android phones, restricting access to particular apps usually requires going onto Google Play. From there, it's fairly easy to navigate your way through the settings to manage the parental controls and authentications relating to any apps on the device. These features can prevent your child from downloading or buying anything unsuitable for their age. Updated versions of apps or games that your child has already installed may occasionally contain something inappropriate, so we've explained how to stop those, too.







How to Block App Downloads (This Also Disables In-app Purchases):

1. Open Google Play Store
2. Tap the profile icon in the top right
3. Tap Settings
4. Scroll down to the Family section and tap Parental controls
5. Toggle 'Parental controls are off' to 'Parental controls are on'
6. Create a PIN and tap OK
7. Confirm your PIN and tap OK again
8. Tap Apps & Games
9. Set the age limit you wish to set
10. Tap Save to apply your changes

How to Stop Auto-updates

1. Open Google Play Store
2. Tap the profile icon in the top right
3. Tap Settings
4. Tap Auto-Update Apps
5. Select 'Don't auto-update apps' and then tap Done

Restricting Apps Through Google Family Link

1. Open Google Play Family Link for parents
2. Tap the three horizontal lines in the top left
3. Select your child's account
4. Tap Manage
5. Tap Controls on Google Play
6. Tap Apps & Games
7. Select the age limit you wish to set

National Online Safety®
www.nationalonlinesafety.com

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 issue of many which we believe trusted adults should be aware of. Please visit www.nationalonlinesafety.com for further guides, hints and tips for adults.

How to Set up PARENTAL CONTROLS for APPS

iPhone

Apple devices come with built-in apps already available: Mail, FaceTime and Safari, for example. However, you can choose which apps and features appear on your child's device and which ones don't. You can also manipulate the features in Game Centre to enhance your child's safety and privacy when playing games, as well as blocking iTunes or App Store purchases if you wish.

How to Restrict Built-in Apps/Features

1. Open Settings
2. Tap Screen Time
3. Tap Content & Privacy Restrictions
4. Tap Allowed Apps (you may need to toggle this to 'on' at the top)
5. Enable or disable the apps you wish to appear (or disappear) on your child's device

How to Restrict Game Centre

1. Open Settings
2. Tap Screen Time
3. Tap Content & Privacy Restrictions
4. Tap Content Restrictions (you may need to switch the toggle at the top to the 'on' position)
5. Scroll down to Game Centre
6. Choose between Allow, Don't Allow, or Allow with Friends Only in the settings for each feature

How to Restrict iTunes & App Store Purchases

1. Open Settings
2. Tap Screen Time
3. Tap Content & Privacy Restrictions
4. Tap iTunes & App Store Purchases
5. Select Allow or Don't Allow for each feature (you can also lock these settings with a password)

National Online Safety®
www.nationalonlinesafety.com

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 issue of many which we believe trusted adults should be aware of. Please visit www.nationalonlinesafety.com for further guides, hints and tips for adults.

What Parents and Carers Need to Know about

APPLE GUIDED ACCESS

iPhones and iPads don't offer separate user accounts. So when you hand your Apple device to a child to play a game or watch a video, you're also handing them access to your email, the web, messaging and numerous other apps through which they could accidentally do something regrettable.

Apple Guided Access solves this potential problem by letting you restrict the iPhone or iPad to one particular app whenever your child uses the device. If they try and leave that app, they will be asked for a password or Face ID, meaning they can't access anything they shouldn't elsewhere on the device. Here, we show you how to find and set up the Guided Access feature, so you can confidently let your child borrow your iPhone or iPad.

How to set it up ...

Step 1
To switch on Guided Access, open your Apple device's Settings – that's the one with the cog icon, normally found on the first of your home screens.

Step 2
In the Settings menu, scroll down and select Accessibility, then scroll down and select Guided Access.

Step 3
Enable Guided Access by tapping the toggle at the top. It should turn green, and a new series of options will appear.

Step 4
You can now customise Guided Access. Under Passcode Settings, for example, you can set a six-digit passcode that must be entered to turn Guided Access back off. You'll also find an option to quit Guided Access using Face ID if your device has that feature.

Step 5
There are audio options, such as scheduling an alert if you decide to set a time limit on Guided Access – to restrict gaming sessions to an hour, say. You can also set an alarm or spoken warning for when the time is almost up, so your child isn't suddenly kicked out of the app. It's a good way to avoid tantrums!

Step 6
Finally, you can alter the length of time before the device auto-locks. If your child is reading on the device's Kindle app, for example, you might want to stop the screen locking after only two minutes of nobody touching it – so they can read happily without interruption. You can select from pre-set time periods or disable the lock function altogether.

How to switch it on ...

Step 1
When you need to start a Guided Access session, open the app your child wishes to use and then press the home/power button or side button on your device three times in quick succession.

Step 2
You can now select parts of the screen that you'd like to lock. If your child's reading on your Kindle app, for example, you could disable the icon that takes them to the main Kindle library – so they don't stumble across books written for an adult audience.

Step 3
The Options menu in the bottom right allows you to set a time limit for the session. Use the scrollable menu to specify the time limit in minutes or hours.

Step 4
Other options in this menu let you control access to settings such as the volume. So if your child's listening to music, you could lock the volume buttons (once it's set to a suitable level) so they can't damage their hearing by playing it too loud.

Step 5
When everything is set up how you want it, click Start. Your child will now not be able to leave that app. If they press the home button to exit, as usual, it will do nothing.

Step 6
The only way to leave Guided Access is to triple-click the home/power or side button (or double-click, if you set up the option to exit via Face ID). Without Face ID, you'll need the six-digit passcode to return to your home screen. Obviously, don't forget that code or let your child find out what it is!

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 the *ITV News at Ten*. He has two children and has writes regularly about internet safety issues.

SOURCES: https://support.apple.com/en-gb/HT202612

National Online Safety®
#WakeUpWednesday

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 game of many which we believe trusted adults should be aware of. Please visit www.nationalonlinesafety.com for further guides, hints and tips for adults.

What Parents Need to Know about POKÉMON GO

AGE RESTRICTION PEGI 7

Pokémon GO has been among the world's most popular mobile games since its spectacular release in 2016. It's recently enjoyed a resurgence, thanks partly to people combining entertainment and exercise during lockdown. In Pokémon GO – like the Pokémon TV show, trading card series and other video games – players capture, train and battle with their Pokémon creatures: physically exploring locations while using augmented reality via their phone's screen. The game generally provides a positive experience, but there *are* still some safety concerns to consider.

ENVIRONMENTAL HAZARDS

Pokémon GO requires players to visit in-game landmarks like Pokéstops and Gyms. These are often situated at public real-world locations such as churches or post offices. Sometimes, however, they can inadvertently end up being placed in dangerous areas which are unsuitable for children, even when accompanied by an adult: near a construction site or a main road, for example.

STRANGERS & MEETING OFFLINE

Players often cooperate with friends in the game, and there are many online discussion hangouts. As well as sharing tips and info, these groups may arrange to meet offline to catch Pokémon or attend raids (communal events where players flock to the same real-world place for a mass battle). This can put children at risk of being messaged and invited to meet by strangers under the pretence of talking about the game.

DATA COLLECTION

When a player logs into their Pokémon GO account, the game collects personal data about the user and their device. Locations, emails, names, ages and even camera images can all be accessed. What then happens to this information is open to debate. Niantic, the game's developers, maintain that they do not sell user information to third parties – but the fact that they have it at all is a concern, nonetheless.

VISIBLE PROFILES & LOCATION

Pokémon GO players can add each other as 'friends' in the game by sharing their trainer codes. Two trainers who do this can then view each other's information, such as their username. If a username gives any clues to the player's real name or personal details, a stranger may then be able to look them up online. The game also lets users upload images to social media, which could publicly disclose a child's exact location.

IN-GAME PURCHASES

The game uses a currency called Pokécoins, which can be bought for real money (in bundles between £0.79 and £99.99) and exchanged for in-game items such as Pokéballs and berries. It's extremely easy for a child to purchase Pokécoins (even accidentally) if there's a payment method connected to their mobile phone – and possibly rack up a sizeable bill without realising it!

Advice for Parents & Carers

PLAY ALONGSIDE YOUR CHILD

Finding and catching Pokémon with young ones could turn into a great mutual hobby. At 25 years old, it's one of the few games franchises that spans two generations. Enjoying the game together will give you plenty of new things to talk about with your child – and if you played Pokémon in your own childhood, you might impress them with your knowledge of the digital critters!

ENCOURAGE AWARENESS

Remind your child of the physical dangers they could face while catching Pokémon and emphasise staying aware of their surroundings. The game will often alert children (through their phone) when they are close to an interesting Pokémon item – usually sending them excitedly rushing off to find it – so they should never play Pokémon GO near busy roads or in places they don't know well.

DISGUISE THE EXERCISE

One of Pokémon GO's benefits is that it encourages young (and not-so-young!) ones to get exercise outdoors. Some parts of the game can be completed from home, but it's best experienced while walking around your local area. Certain tasks (like visiting Pokéstops) can be repeated every day – and an hour outside having fun catching Pokémon will hardly feel like exercise at all!

USE AN OLDER PHONE

If children use an older phone to play Pokémon GO, then they won't be walking around with their own new device, which could get broken or stolen. Parents are also far less likely to have left a credit card linked to the old mobile. It also means that you can limit the amount of information used to set up an account, and what companies who gain access to your data can do with it.

AGREE PLAY BOUNDARIES

Ensure your child knows where they are (and aren't) allowed to go searching for Pokémon, when they have to be home, and how often they can play the game. Talk to other young Pokémon GO fans' parents or carers to see what boundaries they set for their children. Lunchtimes (if allowed by the school) or after school are ideal times for getting some exercise and catching all those Pokémon!

Meet Our Expert

Mark Foster has worked in the gaming industry for several years as a writer, editor and presenter. He is the gaming editor of two the biggest gaming news sites in the world: UNILAD Gaming and GAMINGbible. Having started gaming at a young age with his siblings, he has a passion for understanding how games and tech work – but, more importantly, how to make them safe and fun.

National Online Safety®
#WakeUpWednesday

SOURCES: https://heimdalsecurity.com/blog/is-pokemon-go-safe/
https://bleedingcool.com/games/pokemon-go-announces-quality-of-life-updates-for-february-2021/

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 game of many which we believe trusted adults should be aware of. Please visit www.nationalonlinesafety.com for further guides, hints and tips for adults.

What Parents and Carers Need to Know About...

ROCKET LEAGUE

Age Restriction
PEGI 3

Rocket League is a free-to-play multiplayer vehicle football game. It was developed by Psyonix, now part of the Epic Games family (which also includes Fortnite and Gears of War). Rocket League is essentially a football game where, instead of running, the players drive rocket-powered cars. The game was a surprise hit that took the world by storm when it first released in 2015. Rocket League is available for the Xbox One, Xbox Series X, PlayStation 4 & PlayStation 5, Nintendo Switch, Windows PC, MacOS and Linux.

Fiercely Competitive Community

Competitive gaming isn't necessarily bad. However, playing purely to win (as opposed to simply having fun) can result in aggressive behaviour among some players if they're not successful in the game. Certain people can become hostile or "toxic" towards other players. Continually seeing this behaviour can cause children to think it is acceptable and lead to anger issues while playing.

Unsuitable Online Interactions

18+

A video game's age rating cannot take player-generated elements into account. Rocket League is rated PEGI 3, but its online features mean that appropriateness can't be guaranteed. Audio and text chat, player usernames, player-to-player trades and other user-created content may not be suitable for young players. The game *is* moderated, but catching everything can be difficult.

Grinding and Increased Screen-time

Features like the Rocket Pass and the ranking system can make Rocket League a grinding-focused game. This means players need to spend a lot of time on the game to progress through levels and collect rewards. Grinding encourages regular long gaming sessions for players seeking to climb the rankings (meaning increased screen time) but it doesn't always result in making much headway.

Scams and Bad Trades

Player-to-player trading is common in Rocket League. The game has lots of cosmetic items to collect, and some can be very valuable. Players can trade items among themselves, but younger gamers are not always the best judges of what constitutes a fair deal. This can lead to them being swindled in trades – or to children signing up to illegitimate trading websites, where they then get scammed.

In-App Purchasing

Free-to-play games (so called because they don't cost anything to download) like this depend on players making in-game purchases to turn a profit. Rocket League's in-game currency, called credits, are used to buy items in the game. Credits can be earned by playing the game or can be bought with real money – which could prove expensive if a child lets their love of the game and desire to progress get the better of them.

Advice For Parents & Carers

Use Parental Controls

Psyonix *has* added some safety measures into the game. The text and voice chat can be disabled, for example, limiting contact from strangers. However, it's not currently possible to block contact from other players about trades. It's a good idea, then, to talk with your child about the possibility of scams and bad trades either before they download the game or early in their Rocket League 'career'.

Stay Aware of Spending

Free-to-play games can become money sinks without children realising. For peace of mind, make sure you don't have any payment methods attached to your child's gaming account to avoid accidental purchases. Rocket League credits can be earned through gameplay or bought with real money: encourage your child to use their earned credits first before they ask you to top them up.

Monitor Gaming Time

It's impractical to sit and watch your child every time they play Rocket League. Keeping an eye on their gaming hours is crucial, however: it's easy to lose track of time while playing (even for adults), so "one more game" can soon turn into ten more games. Helping your child to balance their gaming time with their homework, chores and other activities is a life lesson in time management.

Encourage Regular Breaks

Sitting in the same position all day while gaming isn't healthy, but it is an easy habit to fall into. A short break every hour or half hour is important. It allows players to rest their eyes, brains, hands and arms. Learning the value of an occasional break from *any* activity is good practice for the future. Encouraging your child to rehydrate regularly can also help to lower any rising competitive tempers!

Meet Our Expert

Clare Godwin (a.k.a. Lunawolf) has worked as an editor and journalist in the gaming industry since 2015, providing websites with event coverage, reviews and gaming guides. She is the owner of Lunawolf Gaming and is currently working on various gaming-related projects including game development and writing non-fiction books. With experience in esports and content creation, Clare has seen the benefits *and* drawbacks of all aspects of gaming.

National Online Safety®
#WakeUpWednesday

SOURCES: https://support.rocketleague.com/hc/en-us/articles/360015613074, https://support.rocketleague.com/hc/en-us/articles/360053542814-Parental-Controls, https://support.rocketleague.com/hc/en-us/articles/360039907693-How-can-I-protect-my-child-from-online-interactions-, https://theglobalgaming.com/rocket-league/credit-system-free/

What Parents and Carers Need to Know about ...

SOCIAL MEDIA SCAMS

On any social media platform, you'll often come across links to genuine-looking websites. They might include an exclusive offer for one of your favourite shops or invite you to complete a quiz in return for a particular reward. In some cases, clicking on these links takes you to a fake website where you are asked to provide your personal details. The whole enterprise is a ploy to capture sensitive details, such as your email address and password, which the scammers then exploit at your expense.

Clickjacking for fake rewards

Here, the attacker tries to lure you into clicking a link by offering something in return, such as a free gift for completing a survey. However, when the link is clicked, it collects the details of whoever fills out the survey. This might include full names, addresses, phone numbers and email addresses. Scammers could use these to hack into your other accounts or simply sell your data to other criminals.

Malicious app downloads

Some cybercriminals design software that appears genuine or helpful (and is normally free) but has been created to steal your personal information. There may be a pop-up ad encouraging you to download and install the app. Once the app is downloaded, the attacker can see any personal credentials you enter, and could then use this information for their own gain.

'Payment first' scams

Prevalent on sites such as Depop, these scams have spread to Facebook since it added the Marketplace feature. A user lists an item for sale and requests payment up front. Most online stores work this way, but the crucial difference is that scammers ask for payment via PayPal friends and family – not goods and services. This means you can't dispute the payment: the scammer keeps your money, and you never receive the item.

Threats disguised as quizzes

Most quizzes on social media seem harmless, but many come with hidden threats. When you submit your answers, you're also agreeing to terms and conditions which – in some cases – allow the quiz developer to sell your details to third parties. This puts you at greater risk of phishing attacks and spam advertising emails. It might also give the app permission to use information from your profile.

Untrustworthy URLs

It's common on social media for URLs in posts to be shortened (to meet Twitter's character count, for instance). This may seem harmless, but it opens an avenue of attack for scammers who may be disguising a malicious link as legitimate. These links can install malware on the victim's device, which could lead to passwords being stolen or even be the precursor to ransomware attacks.

Angler phishing scams

Using a fake corporate social media account, the scammer pretends to be from customer services. When someone complains about customer service on social media, the fake account messages them asking for their name, phone number and email. If the user provides this info, they are directed to a fake website where they enter their login details. The attacker can then steal their credentials or infect their device with malware.

Advice For Parents & Carers

Set strong passwords

Always ensure that your passwords are not easily guessable. Try to use a mix of letters, numbers and special characters so that criminals cannot forcefully get control. You should also change your passwords every so often to provide further protection against your accounts being taken over. If you have any concerns about your account's privacy, change the password.

Review your privacy settings

Regularly review your privacy settings on social media. You can restrict which parts of your profile can be seen and by who. We recommended making your personal information only visible to friends, which will help to limit the information a scammer could find out about you from social media. It's also safest to only accept friend or follow requests from people that you actually know.

Protect your personal information

Never enter personal information on unfamiliar websites. If you were redirected to a site from a social media post or an email link, putting in your personal details could give key information away to a scammer. Fraudsters may pose as someone you know to try and get your address or bank details (or your family's). If this happens, block the user and tell your family, so the scammer can't try to deceive anyone else.

Avoid opening suspicious emails

When you get an email, always check the sender's address before opening it. If it's an unexpected email and the sender is a stranger, mark it as junk (in case they try again in future) and simply delete it. They could be a scammer who's simply seen your email address on your social media profile. Being aware of phishing attacks is the primary method of defence against scam emails like this.

Choose trusted download sources

Don't download apps or files from unknown sites – instead, use verified and trustworthy sources (such as Google Play or the App Store for download to mobile devices). You can recognise safe sources by their trust seals. The browser address bar on a secure site starts "https" instead of "http". A shield or lock symbol in the address bar also indicates that a site is secure.

Install anti-virus software

Another key tip is to ensure that you have robust and reliable virus protection installed on any of your devices that support it. Anti-virus programmes will help to insulate you against cyber-attacks by blocking any malicious downloads or detecting any recently downloaded malware and removing it. Update your virus protection software regularly and carry out frequent scans of your device.

Meet Our Expert

Formed in 2016, KryptoKloud provides cyber security and resilience solutions to its customers. With offices in the UK, the company offers managed service operational packages including cyber security monitoring and testing, risk audit, threat intelligence and incident response.

KryptoKloud

National Online Safety®

#WakeUpWednesday

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 issue of many 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 EMAIL SCAMS

Email scams are when you receive a mail from someone purporting to be a genuine person or company, but is actually an online fraudster trying to trick you into disclosing personal information. This is often referred to as 'phishing'. Normally, people click on the links in an email assuming that they will be directed to a trustworthy website – but fake sites, closely resembling the real thing, are increasingly being set up by cyber criminals specifically to capture your personal information, which could in turn jeopardise your financial, emotional and possibly even physical wellbeing.

Disguised Deceptions

Some scam emails can appear to be from companies that you know and use. For example, you could receive an authentic-looking email advising of a problem with your account or payment method. Instead of reacting to the email and disclosing personal information like bank details, it's wise to call the company directly on a trusted number to confirm if there actually *are* any account issues.

Identity Theft

Another significant risk is falling victim to identity theft. If a scammer manages to acquire your usernames and passwords, they would then have access to your online accounts – and they could effectively pretend to be you. This could have a massive negative impact if changes were made to your accounts, for instance, or the scammer communicated with your contacts while posing as you.

Viruses and Malware

A particularly devasting hazard with scam emails is that some links, when clicked on, could result in dangerous viruses or malware being downloaded onto your devices. This could enable scammers to harvest valuable information without your consent (and sometimes even without your knowledge) or prevent you from accessing the device altogether, making it unusable.

Financial Damage

One of the primary consequences for victims of an email scam is the financial cost. If you *do* click on a scam email and disclose any personal information, it can then be used to take money from accounts belonging to you and your family. Depending on exactly what information the cyber criminals obtain, this could result in significant and far-reaching financial losses and personal stress.

Hijacked Accounts

A scammer with access to your accounts could – once they're logged in as you – deny you entry. If they were to change the password, it would – in most cases – not allow you any further access. Even for accounts with little or no financial value attached, this could be hugely inconvenient: you could permanently lose data and files that you had invested a considerable amount of time in.

Personal Safety

Another danger of scam emails is that, in extreme cases, they could ultimately lead to a threat to your physical wellbeing. If someone is demanding to meet with you and has accessed your personal information (your address, for example), they could attempt to confront you in person – which is of course exceptionally dangerous. Losing control of sensitive information could put you in a vulnerable position.

Advice for Parents & Carers

Protect Personal Details

Never input any personal information into websites that you are unfamiliar with. If you were redirected onto a certain page by clicking a link in an email, entering your personal details could then give away your location or other key information to the scammer. This could then put you in physical danger as the cyber criminals would know exactly where to find and approach you.

Beware of Suspicious Emails

If you are unfamiliar with the sender, it's safest to simply not open an email. When an email makes you wary, mark it as junk (to reduce the chance of any recurring issues) and then delete it. Awareness of phishing is the primary method of defence against malicious emails. Once someone knows how to identify and deal with scam emails, they are far less likely to fall prey to them in future.

Check Spelling and Grammar

Pay close attention to any spelling mistakes or grammatical errors. Many scam emails can be spotted this way, as they often tend to contain these types of mistakes. Make sure your child knows that if they *do* spot this sort of tell-tale error and is not sure who the email came from, it's a good idea to either delete the email or report it to a trusted adult to prevent any possible future harm.

Access Sites Manually

If you or your child wish to visit a particular website, it's safest to avoid clicking on a link in an email to take you there. Instead, find the site through your search engine or manually type the address into your browser. This significantly reduces the possibility of being redirected to a bogus website where fraudsters could capture your personal information after you enter it.

Don't Open Dubious Attachments

If you or your child ever see any files as attachments on emails that you are uncertain about, do not download them or even click on them: this could result in your systems being infiltrated. If your devices at home do not already have anti-virus software, you should install some and ensure it is regularly updated. This will help you to detect and remove any dangerous files as soon as possible.

Meet Our Expert

Formed in 2016, KryptoKloud provides cyber security and resilience solutions to its customers. With offices in the UK, the company offers managed service operational packages including cyber security monitoring and testing, risk audit, threat intelligence and incident response.

KryptoKloud

National Online Safety®

#WakeUpWednesday

SOURCES:
https://www.infosecurity-magazine.com/news/education-disproportionate-spear/, https://www.vumpactmyth.com/blog/cybersecurity-in-education-stats-2020/

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 issue of many which we believe trusted adults should be aware of. Please visit www.nationalonlinesafety.com for further guides, hints and tips for adults.

10 Top Tips for ...

KEEPING CHILDREN SAFE FROM CYBER CRIME

We all want to continue being informed and inspired by the ever-expanding capabilities of the internet. But we also need to be able to safeguard ourselves against the growing amount of online hazards. Knowing what is fact, understanding what dangers exist and taking appropriate steps can go a long way towards protecting yourself and your family. National Online Safety has collaborated with the Yorkshire and Humber Regional Cyber Crime Unit to compile 10 pointers to help you keep your children safe from cyber crime.

1. Spot Phishing Bait

Phishing messages are untargeted mass emails asking for sensitive information (e.g. usernames, passwords, bank details) or encouraging recipients to visit a fake website. It's safest to learn the warning signs of phishing and increase your child's awareness. Too good to be true? Spelling or punctuation errors? Odd sense of urgency? These are all red flags. Don't click on links or follow demands: if you're unsure, contact the official company directly online to enquire further.

2. Don't Over-Share

Is your child sharing too much on social media? Do they post things about their private life, upload images of your home, or discuss their friendships and relationships online? Criminals will gather this information and may try to use it for identity theft or other offences such as fraud. To combat this, ensure your child's privacy settings mean they are only sharing information with family and close friends. Use parental controls where appropriate.

3. Encourage Strong Passwords

Weak passwords make it faster and easier for someone to gain access to your online accounts or get control of your device – giving them a route to your personal information. For a strong password, national guidance recommends using three random words (e.g. battlegaragepylons). Consider paying for your child to access a password manager. Encourage them to have a separate password for their email account. Ensure the whole family uses two-factor authentication where possible.

4. Stay Updated

People often put off installing updates to apps or software because they don't feel it's necessary, it can be time consuming, or could cause problems with programmes they rely on. But updates help protect users from recently discovered vulnerabilities to malware. You can usually set them to run automatically – encourage your child to select this option. Ensure updates are installed as soon as possible after you're notified they're available.

5. Back up Your Data

Some cyber attacks can lead to the theft or deletion of important (and possibly sensitive) data or loss of files (like photos and videos) that can't be replaced. Backing up your data to the cloud – or to another device – will help prevent data loss if you ever become the victim of a cyber attack. Where possible, set your child's devices to back up automatically. Also encourage them to back up their data prior to installing any updates.

6. Be Wary of Public WiFi

Free public WiFi is commonplace – but it's often not secure and sends unencrypted data via the network. A hacker on the same network could access personal data (like financial information) without you even realising they'd done so. To avoid this, suggest to your child that they use their 3G or 4G mobile data when they're out and about, rather than free WiFi. Consider purchasing a VPN (Virtual Private Network) where possible.

7. Take Care When Chatting

Criminals may look to manipulate others online and coerce them into using their talents or cyber skills for unethical means. Try to get your child to be open about who they are talking to online. Communication tools such as Discord are popular among gamers – but be cautious of the other people using them, and ensure you know who your child is chatting with.

8. Recognise Warning Signs

Often, budding cyber experts will relish the challenge of testing themselves or earning recognition from peers for their exploits. Even principled 'white-hat' hackers will look to test their skills online. If you think your child is interested in hacking, try to understand what their motivation is. You could encourage their participation in ethical competitions such as bug bounties.

9. Understand Their Motivations

Those being influenced online to use their skills unethically may display certain key warning signs. Sudden evidence of new-found wealth (unexplained new clothes or devices, for example), secrecy around their online behaviour or boasting of new online friendships are all causes for concern. If in doubt, refer through to your regional cyber crime team.

10. Know the Consequences

Many young people may feel that hacking is essentially a light-hearted prank, and not especially serious. So make sure your child is aware of the implications of a conviction under the Computer Misuse Act – not only the possibility of a criminal record, but also lifelong travel restrictions and damage to their future career or educational prospects.

Produced in Partnership with

The Yorkshire & Humber Regional Cyber Crime Unit (YHRCCU) works with the National Crime Agency (NCA) and other partners, in the UK and abroad, to investigate and prevent the most serious cyber crime offences.

YH ROCU

Yorkshire & Humber
REGIONAL CYBER CRIME UNIT

NOS National Online Safety®

#WakeUpWednesday

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 topic of many which we believe trusted adults should be aware of. Please visit www.nationalonlinesafety.com for further guides, hints and tips for adults.

Part of our Online Privacy & Security Series

NOS Online Privacy & Security

10 Top Tips for SAFER ONLINE SHOPPING

1. CHECK IT'S A LEGITIMATE SITE

It's safest to stick with well-known, reputable retailers. If a site doesn't look professional, or has weird pop-up ads, it's best to steer clear – no matter how tempting their prices. If something seems too good to be true, it probably is!

2. MAKE SURE THE SITE IS SECURE

When you're buying online, look for a padlock icon near the address bar – or check if the URL includes "https" or "shttp". The extra 's' or the padlock mean you can rest easy: you're sending your card details and personal info via a secure channel.

3. READ THE SMALL PRINT

Take note of details like a seller's returns policy. It's easy to shop impulsively when you're online and then be stuck with unwanted items because of a very small window for returning goods. Also check delivery estimates if you're buying for a specific date (like a birthday).

4. CREATE SECURE PASSWORDS

When shopping around online, you'll often need to set up an account when buying from a site for the first time. Choose a different password for each: the longer, the better. It's best practice to mix upper- and lower-case letters, symbols and numbers.

5. ACKNOWLEDGE THE ASTERISK

When you register with them, online retailers clearly need some essential info (name, address, payment details, etc), usually marked by an asterisk. Anything else is for marketing purposes or possibly to sell your data. So don't feel pressured into giving those details out.

6. AVOID PUBLIC WI-FI

When you are on the high street, don't use public WiFi to buy things online. It might seem super-efficient to shop on your phone while you're queuing or taking a break – but the WiFi in shopping centres or coffee shops isn't secure. Using 3G or 4G will be slower, but it's safer.

7. REINFORCE YOUR SECURITY

Before you shop, check that your browser and any anti-virus software are up to date. Updates often contain improvements to your device's security. You could also consider using intermediary services like PayPal, Apple Pay or Google Pay, which offer advanced protection.

8. WATCH OUT FOR PHISHING

Retailers regularly send out emails to publicise their latest deals. Hackers often try to use this traffic as camouflage; look out for emails with poor grammar, suspicious reply addresses and pixelated images – they're all signs of an attempt to 'phish' your personal details.

9. PLAN YOUR SHOPPING

Before going online, make a list of what you're in the market for – and stick to it. Because you're not physically putting items in a bag that you then have to carry, it's easy to lose track of how much you've bought and end up with a massive over-spend by the time you log off.

10. READ THE REVIEWS

We've all bought something which sounded amazing online, only for it to be far less impressive when it actually arrived. Take time to read other buyers' views on an item – and think twice about anything that only has a small number of comments about it.

National Online Safety®

#WakeUpWednesday

SOURCES:
https://www.statista.com/topics/871/online-shopping/