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. bottlegaragepylons). 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

National Online Safety®

#WakeUpWednesday

www.nationalonlinesafety.com @natonlinesafety /NationalOnlineSafety @nationalonlinesafety

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 10.02.2021

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 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 CLUBHOUSE

Clubhouse
Drop-in Aud

17+
App Store Rating

Clubhouse is an audio-only social media networking app that is currently available only to Apple users. The app encourages conversation between users, in various rooms discussing topics from the serious (health, sports, cryptocurrency, etc) to the more frivolous (favourite cereals, corniest jokes and so on). Clubhouse is like an interactive podcast that allows real-time two-way communication. The app is still in beta-testing stage and is invite only – you can only join if someone sends you an invite.

Fear of Missing out

Clubhouse's exclusivity has created significant curiosity and FOMO ('fear of missing out') among internet users still awaiting their invite. Many have turned to Reddit forums and social media for a way in. Scammers are exploiting this excitement: there have been people with the same username selling invites on different platforms. This is a red flag, since any one person only gets two invites to use.

Lack of Moderation

Clubhouse wants to be a safe environment for its users and aims to assign a moderator to every room. However, as users are able to create their own rooms at will, it is hard to see how all of these could be appropriately moderated. Hence, a young person listening in could easily be exposed to adult language or comments that could be deemed offensive.

Recorded Conversations

There has been no evidence to date of Clubhouse conversations being leaked onto the wider internet. But the possibility cannot be dismissed that someone could easily record a conversation and then circulate it online. This would become a problem if a young person used their real name on the app and discussed a potentially sensitive issue in any of the rooms.

No Age Verification

+18

The app is targeted at users aged 18 or over. However, there is no age verification system in place (as yet), so anyone under 18 could easily join the app if they received an invitation. As Clubhouse encourages forthright discussion among adults, a young person signing up to the app would be highly likely to hear vigorous discussions of age-inappropriate subjects.

Insufficient Safety Protocols

Although the app condemns hate speech and online abuse – and is working hard to keep these off the platform – there *have* been some safety concerns about Clubhouse. The speakers in some rooms, for instance, have been found to be taking advantage of the lack of moderation to incite hate against minority groups.

Accidental Exposure

There are three types of room: open (anyone can join), social (only for someone's 'friends' on the app) and closed (the room creator decides who is allowed in). A child could easily be invited to join rooms by their friends or by someone they follow. This may result in them accidentally joining rooms that aren't age appropriate. There is currently no way to prevent this from happening on the app.

Advice for Parents & Carers

Use 'Closed' Rooms

If your child is determined to use Clubhouse, emphasise that – in privately created rooms – they should only chat with people who they actually know. When creating their own chat room, encourage them to always set it to 'closed' (so only they can decide who can listen in or join the conversation) and don't allow strangers to have access.

Block or Report

Even as just a listener you can block someone or report them for abusive behaviour. If your child comes across a speaker in Clubhouse that is being offensive or abusive, then encourage them to block and report that user. It's good practice to always walk your child through blocking and reporting on any app with those facilities, giving them a method to protect themselves.

Emphasise Digital Etiquette

There are no text-messaging or image-sharing options currently available on Clubhouse; speakers whose presentation needs a visual element change their profile picture as a way to show the image. But it is still possible that conversations (even in private rooms) may be recorded by another user. Remind your child of the importance of maintaining good digital etiquette and behaviour.

Avoid Linked Social Media

When creating a profile, users can link it to their Twitter or Instagram account. Many people have used this to then connect with or message others users directly. You can protect your child's personal information by keeping any other social media accounts they might have separate from Clubhouse. This will reduce the potential of a stranger privately messaging your child away from the app.

Talk about the App

Clubhouse is for over 18s. So if a young person really *does* want to use the app, assess whether they are mature enough to handle some of the conversations they might encounter before allowing them to download it. Prevent them being misinformed by encouraging them to research the speakers they follow – making sure that they are credible people who are qualified to present on a particular topic.

Explore It Yourself

If your child is interested in Clubhouse, perhaps the best way to understand how the app works, and its format and content, is to download it yourself before they do. Trying the app will help you to decide if it is appropriate for your child to use. If you're not happy that it's suitable, explain your reasoning to your young one and possibly cooperate in researching more child-friendly alternatives.

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.

NOS National Online Safety®
#WakeUpWednesday

https://www.indiehackers.com/product/clubhouse-invites/reddit-clubhouse-invite-dont-buy-clubhouse-scams--MRZGgMG_OOZQIKmLuEf
https://www.bloomberg.com/news/articles/2021-01-26/as-tech-darling-clubhouse-grows-so-does-scrutiny#:~:text=A%20Clubhouse%20spokeswoman%20said%20racism,flag%20rooms%20for%20further%20investigation.

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 24.02.2021