Managing Your Online Reputation

WATCH_YOUR_SPACE CHECKLIST

CHECK YOUR SETTINGS

Some of the most popular social networks are set to public by default, meaning everyone can see our photos, what we are sharing or talking about. Regularly check your privacy settings across your social networks and apps. We recommend a 'friends only' option for your online profiles.

SEARCH FOR YOURSELF ONLINE

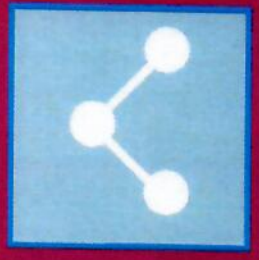
Do a quick search for yourself online, if you find something you don't like report it with the website or network host requesting the content be removed.

DEACTIVATE OLD ACCOUNTS

Social media changes so quickly, it can be easy to forget about old accounts or networks we've signed up to. If you're not using an account delete/deactivate it, this can help avoid risk of accounts/profiles being hacked.

MAKE THE MOST OF YOUR TIME ONLINE

What we do online can follow us around, ensure you make a positive impact. Whether it's starting a blog, raising awareness for something you care about or becoming the next Mark Zuckerberg... the possibilities are endless!



THINK BEFORE YOU POST

Before you share, comment, like, post, Tweet or pin anything... ask yourself if this is something you want everyone to see? Use the **THINK** model if you're unsure about posting something online >>> Ask yourself is it **T**rue? Is it **H**elpful? Is it **I**llegal? Is it **N**ecessary? Is it **K**ind?

AGE RESTRICTION

13+

Snapchat is a photo sharing app for mobile phones and tablets. The app allows users to share images, videos and chat with friends. Users can share images and videos directly to specific friends, or through a 'story' shared with their entire friend list, which documents the previous 24 hours. In a study, Snapchat was ranked the 4th most negative app in terms of having an impact on young people's health and wellbeing, with children feeling that they can use the app Snapchat to "make you look pretty."

What parents need to know about SNAPCHAT

EXPOSING YOUR CHILD'S EXACT LOCATION

The 'Snap Map' lets you share your EXACT location in real-time through a map on the app. The user's location updates when the app has been opened on the device. There is a warning on the Snapchat website about uploading images and videos to 'Our Story' stating that "snaps you submit to 'Our Story' can still show up on the Map, no matter which location setting you choose." When uploading to 'Our Story,' your child's image or video could appear in "Search results and Stories on or off Snapchat – today or in the future."

LENS EXPLORER

The 'Lens Studio' on Snapchat gives users the freedom to use their imagination to design their own filters for themselves and others to use. Snapchat states that the lenses users create "must comply with our Lens Studio Submission Guidelines and Community Guidelines and must be appropriate for Snapchatters ages 13+." The 'Lens Explorer' in the app now enables users to choose from thousands of these creations to alter their snaps. Anyone can create a lens for Snapchat, which gives opportunities for age-inappropriate content to be uploaded.

SCREENSHOTS & SAVED MESSAGES

While Snapchat's gimmick is that all photos, videos and text disappear eventually, users still have the capability to screenshot or record anything which has been sent to them. Users may sometimes forget that screenshotting is possible and send a compromising image or message to somebody who they think they trust. They may also accidentally send an image or message to somebody who they do not trust. Simply by pressing and holding a message, the user is able to save a message they have received, which can be screenshotted or used against them at a later date.

SNAPSTREAKS & ADDICTION

'Snap Streaks' are gained when snaps have been sent back and forth consecutively between friends. The longer that snaps are sent between users, the longer the streak becomes. Furthermore, Snapchat rewards users who have achieved high Snap Streaks, by gifting emojis, adding incentives for users to keep the streaks. Children invest time into making their streaks as long as possible, which can put an incredible amount of pressure on both themselves and their friendships.

SEXTING

Due to 'Snaps' disappearing, (users can even send a one-second photo or video), Snapchat has become the chosen platform for children and young people to send sexually explicit images or 'selfies.' Once a photo/video has been screenshotted, or recorded using another device or software, this can lead to further dangers, such as blackmail and cyberbullying. It is illegal to make, possess, download, store and share sexual images, photos and videos of a person under the age of 18. This also includes any sexual images, photos and videos that a child may have taken of themselves. However, if a young person is found creating or sharing images, the police can choose to record that a crime has been committed, but taking formal action isn't in the public interest.

SNAP ORIGINALS

Through 'Snap Originals,' users can watch content which has been created by Snapchat on the app, including comedy shows, drama, news and more. Additionally, there are new lenses and filters available, inspired by the 'snap originals' shows. This is another feature to encourage addiction.

Top Tips for Parents

THE RISKS OF SEXTING

It can be slightly awkward talking about this topic with your child, but if it helps them protect themselves, it is worth it. Talk to them about the consequences of sexting and make sure that they're aware of the risks. Ensure your child knows that 'Snaps' can be screenshotted. Teach them that if they post anything potentially embarrassing or harmful (either of themselves or someone else) it can have severe consequences as the message, image or video can be shared further.

REPORTING A STORY, LENS, FILTER, SNAP OR MESSAGE

If your child comes across inappropriate Snapchat content sent directly to them or in another person's story, advise them to report it immediately. This may include an inappropriate lens, filter, message or snap. To report an offensive lens, they should open the app and select the lens they want to report. An info button will appear above the lens. Click this, followed by the flag icon. This will send a report to Snapchat for further investigation. Reports can also be made on the Snapchat support website: support.snapchat.com.

USE 'GHOST MODE'

We highly recommend enabling 'Ghost Mode' on the app so that your child's location will no longer be visible to anyone on the 'Snap Map.' To enable this, go onto the Snap Map and tap the cog in the top-right corner. Here, change the setting to 'Ghost Mode.'

HOW TO DELETE A MESSAGE

Advise your child never to send any negative messages (or images through gallery in the chat on the app) as screenshots can still be taken. You should also advise your child to screenshot any negative comments they receive as the sender can also delete them. To delete a message, simply press and hold the sent message and press delete.

TURN OFF 'QUICK ADD'

'Quick Add' helps friends find each other on the app. This is based on mutual friends or if their number is in their phone book. Explain to your child that this feature can open up their profile to strangers. We highly recommend that your child turns off the 'Quick Add' feature. This can be done in the settings.

RESTRICT STORY VIEWS

Your child can add videos and images to their 'Story' throughout the day which will last for 24 hours. By default, anyone in a user's friends list can see their story. We recommend checking the privacy settings to ensure that this has not been edited. This can simply be done in the apps settings under the 'Who Can View My Story' section. The options to choose from are 'My Friends,' 'Everyone' or 'Custom' - we suggest that it is set to 'My Friends.'

National Online Safety

A whole school community approach to online safety

www.nationalonlinesafety.com

Email us at hello@nationalonlinesafety.com or call us on 0800 368 8061

Mind: Social media and young people's mental health | Life in Likes - Childrens Commissioners Report | Google Play Store | https://support.snapchat.com/en-GB
https://net-aware.net/snapchat-parent-review/ | BT.com | Independent.co.uk

At National Online Safety we believe in empowering parents, carers & 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 & tips for adults.

YouTube

AGE RESTRICTION 13+

YouTube is an online platform - owned by Google - where anyone can upload & watch video content. All different types of information, advice & entertainment are uploaded & billions of people tune in to watch, rate & comment on it. As a parent, it's important you understand exactly what content your children might be seeing.

What parents need to know about YOUTUBE

INAPPROPRIATE CONTENT EASY TO ACCESS

Any child with a Gmail account can sign into YouTube & access videos. Some content is flagged 'age-restricted', but the platform relies on self-verification, meaning kids can get around the rules with a fake date of birth. This could enable access to vulgar, violent & dangerous videos.

USERS CAN PRIVATELY CONTACT YOUR CHILD

When your child is signed-in to YouTube with their Gmail account, there are various ways they can send & receive messages. This could be via the messages icon, or via the 'About' tab. There is scope here for users who your child does not know to make contact.

YOUTUBE SUGGESTS RELATED CONTENT

YouTube will often 'auto play' videos based on your child's viewing habits. The aim is to show related & appropriate content. But the problem is: it's possible your child will be exposed to inappropriate content that isn't accurately related.

'CHALLENGE VIDEOS' CAN GO TOO FAR

Challenge videos refer to a stunt you're encouraged to recreate & film. Many challenge videos can be harmless & for a good cause, like the Ice Bucket Challenge. But some are dangerous & even life threatening, such as the Bird Box Challenge.

SHARING VIDEOS RISKS YOUR CHILD'S PRIVACY

If your child has a Google account, they can upload their own videos. To do this, they must create a personal profile page known as a 'YouTube Channel'. The videos uploaded here can be viewed, commented on & shared by anyone. This could put your child's privacy at risk.

SHARE

Tips To Protect Your Child

APPLY 'RESTRICTED MODE'

Restricted mode helps to hide any mature or unpleasant videos from your children. It uses YouTube's own automated system & looks at what other users flag as inappropriate content. It must be enabled in the settings menu on each individual device.

CHANGE WHO CAN SEE VIDEOS

You can change who can view your child's content in the settings. Options include Public (available to all), Private (only available to people you share it with & cannot be shared) or Unlisted (available to people you share it with & can be shared further).

BLOCK CONCERNING USERS

To help protect your child from cyber bullies, harassment or persistent offensive comments, you can 'block' individual users. Doing so hides your child's videos from the user & stops the user being able contact your child in any way.

CUSTOMISE THEIR EXPERIENCE

Influence & control what your child watches using features such as Playlists (your videos play continuously rather than videos YouTube recommends) & Subscriptions (you choose channels your child can watch). It's also good to turn off auto play by toggling the blue button alongside the 'Up Next' title when viewing a video.

CREATE A 'FAMILY' GOOGLE ACCOUNT

Create a Google account to be used by the whole family. This will allow you to monitor exactly what your child is watching, uploading & sharing. Plus, your child's YouTube page will display their recently watched videos, searches, recommended videos & suggested channels.

GET YOUR OWN ACCOUNT

Create your own account so you can explore features yourself. Learn how to flag inappropriate videos, how to moderate comments & how to block users. This will help you feel more confident when providing advice & guidance to your children.

BE MINDFUL OF CYBERBULLYING

Once your child has posted a video, a worldwide audience can see it. Strangers may choose to comment on the video, both positively & negatively. So, be careful to check comments & any other interactions your child is making through the platform.

GET TO KNOW POPULAR CHANNELS

It's good to know which channels are most popular with your children. Some of the most popular channels right now are: PewDiePie, NigaHiga, Zoella, KSI, JennaMarbles, Markiplier, Smosh, ThatcherJoe & Casper Lee.

DON'T ASSUME YOUR CHILD IS TOO YOUNG

YouTube and YouTube Kids are quickly becoming the chosen viewing platforms for children between the ages of 3-15 & it's likely this trend will only increase. It's also possible children will become familiar with the platform at a younger & younger age. So it's important to understand the positives & negatives of the platform.

National Online Safety®

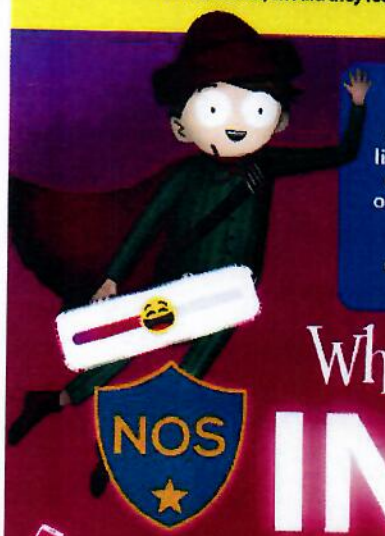
#WakeUpWednesday

Meet our expert

Pete Badh is a writer with over 10+ years in research and analysis. Working within a specialist area for West Yorkshire Police, Pete has contributed work which has been pivotal in successfully winning high profile cases in court as well as writing as a subject matter expert for industry handbooks.

SOURCES: https://support.google.com/accounts/answer/1350409, https://support.google.com/youtube/answer/6401182, https://support.google.com/youtube/answer/2802272?hl=en-GB, https://support.google.com/youtube/answer/7354993?hl=en-GB, https://www.youtube.com/intl/en-GB/yt/about/policies/#community-guidelines, https://www.ofcom.org.uk/__data/assets/pdf_file/0024/134907/Children-and-Parents-Media-Use-and-Attitudes-2018.pdf, https://www.raisingdigitalnatives.com/youtube-parenting/, https://www.net-aware.org.uk/networks/youtube/, https://www.theguardian.com/technology/2019/jan/16/youtube-bans-dangerous-pranks-after-bird-box-challenge

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.



Instagram is a hugely popular social networking app with over 1 billion snap happy users worldwide. The app, which is accessible on iOS and Android devices, allows users to upload images and videos to their feed, like an online gallery. Images and videos can be transformed with an array of filters to edit the shot before sharing. 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. The app has additional features like an 'Explore Page,' which contains videos and images tailored to each user based on accounts and hashtags they follow.

Publish date: 23/05/18
Edit date: 06/03/19

AGE RESTRICTION 13+

What parents need to know about INSTAGRAM

HOOKED ON SCROLLING

Instagram revealed that young users spent a minimum of 32 minutes on the app per day. Many social media platforms, Instagram included, have been designed in a way to keep us engaged on them for as long as possible. Behavioral 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 scrolling until they find that 'something' they are looking for. Children may quickly lose track of time as they get deeper into their Instagram feed.

SLIDING INTO DM'S

Direct messages (or DM's) 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. Dr Danielle Wagstaff, a psychology professor from Federation University Australia, said that social media and influencer culture can sometimes lead us to "derive a false sense of what everyone else is doing" and that this "can definitely have a negative effect on our mental health and wellbeing."

DAMAGE TO CONFIDENCE, BODY IMAGE & MENTAL HEALTH

In a recent 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 boss Adam Mosseri promised to ban images of self harm, following the suicide of 14-year-old Molly Russell, who had reportedly been looking at such material on the platform.

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, but this feature can be turned off. 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 February 2019, the NSPCC demanded a crackdown on Instagram's 'failed self-regulation' after it was revealed grooming and abuse via the app had more than tripled. 5,000 cases of sexual communication with children, some as young as 5, took place in 18 months.

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.

EXPSOSING 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. Posting photos and videos is Instagram's biggest selling point, but with sharing images comes risks. 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 not set to private, anyone can access their account and see their location.

HIJACKED HASHTAGS

Like Twitter, hashtags are also an extremely prominent tool in Instagram and with that comes dangers for your child. 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 certainly shouldn't be exposed to.

IGTV

Instagram TV (IGTV) works similarly 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

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.

LOOK OUT FOR #ADS

In January 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.

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.

SCROLLING

Instagram added a 'You've completely caught up' message in late 2018. This message breaks up the feed and notifies you when you are up to date and there are no more new posts from followers. This features is enabled automatically, but have the conversation with your child about how much time they are spending on the app and set healthy time limits.

PROTECT THEIR 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 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.

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 they can take action against the user if necessary. This is an automatic filter, but it can be turned off. Make sure it is turned on in the app's settings.

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.

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

@MENTION

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 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.

Publish date: 03.04.19

In today's digitally connected world, children and adults are constantly presented with new ways to engage, react and contribute. We're sociable beings; it's a natural human instinct, especially amongst younger audiences, to want to belong and join in. Viral Challenges (as they're often known) draw on these emotions and, as the name suggests, spread and gather pace very rapidly. New challenges are constantly emerging and evolving. They're often completely innocent, raising awareness of worthy causes or simply providing amusement. However, they can have much more sinister undertones, putting children at risk of physical harm or, in extreme cases, fatal injury.

What parents need to know about ONLINE CHALLENGES

MENTAL HEALTH & WELLBEING

As well as having the potential to cause actual physical harm, some challenges can be extremely upsetting for children. Many are created with the sole purpose of instilling fear in an individual in order to coerce them into doing things that could have a long-term emotional effect on them.

VARYING LEVELS OF RISK

As a parent or carer, it's important to take a balanced view and understand that not everything online has the potential to do harm. Mass-following and interaction can be a force for good. For example, the Ice Bucket Challenge, which swept the nation, set out to raise money and awareness of Amyotrophic Lateral Sclerosis (ALS). At its height, over 28 million people uploaded, commented on, or liked Ice Bucket Challenge related posts on Facebook. It's equally important to be aware though that online challenges often have a darker side. Malicious trends and challenges can expose children to dangerous or even life-threatening situations, so it's critical that parents and carers are aware of the latest risks and understand what steps to take to mitigate them.

'FOMO' - FEAR OF MISSING OUT

The 'Fear of Missing Out' (FOMO) is a strong emotional characteristic, particularly displayed in young people. The nature of viral challenges encourages children to explore and push boundaries. They tap into FOMO by feeding on a child's natural desire to join in, be accepted and share experiences with their friends and the wider online community. A recent study also found that FOMO is one of the greatest causes of Social Media addiction.

National Online Safety®

STRIVING FOR LIKES

In a major study by the Children's Commissioner, it was found that children as young as ten years old are reliant on 'Likes' for their sense of self-worth. A major concern around viral challenges is not knowing how far children will go to earn 'Likes'. Couple this growing appetite for acceptance with commonplace peer pressure and the potential problem is compounded. The result is that when young people are drawn into online challenges, because it is what all their friends are doing, saying 'no' can seem like a very hard thing to do.

"The coolest person at school will start a trend and then everyone copies her"
Merran, 12, Year 7

"If I got 150 likes, I'd be like that's pretty cool it means they like you"
Aaron, 11, Year 7

Top Tips for Parents

COMMUNICATION & MONITORING

It's important to talk to your child regularly and monitor their online activities. Encouraging honesty and openness, will give you a much clearer viewpoint of how your child is interacting online and what concerns they have. Create an atmosphere of trust. Ensure they feel they can confide in you or another trusted adult regarding anything they may have seen or experienced online that's upset them.

THINK BEFORE ACTING

As with most concerns in life, let common sense prevail when it comes to Viral Challenges. Young people need the freedom and space to explore and going in all guns blazing may well be counter-effective. Address the importance of safety and wellbeing, both online and offline, by getting the facts and understanding the risks. Start a discussion about the Online Challenges that may have captured your child's interest, gauge their likely involvement and explain the importance of thinking and acting independently when it comes to participating.

SETTING UP EFFECTIVE PARENTAL CONTROLS

As with all online activity, ensuring you have effective parental controls set up on all devices will help filter and restrict the dangerous or inappropriate content you don't wish your child to access. Additional measures for protecting your child include checking the privacy settings on your child's devices, monitoring their friends list, ensuring their personal information is safe and secure and keeping a watchful eye on the content they're sharing.

REPORTING & BLOCKING

Parental controls can only go so far in blocking potentially harmful content. A rise in the decoding of social media algorithms, has led to age inappropriate content increasingly appearing on platforms and apps used by children. Where possible, you should regularly monitor what your child sees online and flag/report any content which is inappropriate or dangerous. You should take the time to talk to your child, define what you consider to be appropriate content and show them how to report and block users/accounts themselves.

VALIDATE SOURCES

Not everything is as it seems. Some people create fake content that's designed to 'shock' in order to encourage rapid sharing. If your child has seen something online that has triggered concern you should encourage them to, check its origin, verify that it came from a credible source and check the comments made for any clues to its validity.

FACING REALITY

Trends and Viral Challenges can be tempting for children to take part in; no matter how dangerous or scary they may seem. As a parent or carer it can be difficult to keep pace with the very latest Online Challenges emerging. In recent months these have included potentially dangerous crazes, including the 'Bird Box' challenge, which was inspired by Netflix's popular film and encourages followers to upload videos of themselves attempting everyday tasks while blindfolded. The best advice is to keep talking to your child. Show that your taking an interest and not just prying. Ensure your child knows they don't have to get involved and if they're unsure, let them know you're there to talk before they consider participating. Children often need reassurance that not everything they see online is real. If your child has viewed distressing or frightening content it's important to talk to them about their experience, support them and, if required, help them find additional support.

SOURCES

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.

Smart devices promise to make our lives easier. In many cases - they do, however these new technologies present risks too. Whether you're using a digital assistant to record your shopping list or you're controlling your lights through a smart system, many smart functions can be 'hacked' and controlled by someone outside your home. This guide will help you identify some of the ways you can stay alert and protect yourself.

1 KNOW THE RISKS

The success of any smart device relies on it communicating with other devices using the Internet. It's an unavoidable part of using smart devices, but it does expose you to numerous risks. Attackers could use the Internet connection to steal your data for identify fraud or to make unauthorised purchases through your devices. There is even potential for more sinister exploitation, such as child grooming or cyber-bullying.

2 WHAT IS THE INTERNET OF THINGS?

This is the term given to all the devices connected to the Internet in your home. It includes a new digital doorbell connected to your smartphone, your kettle that boils when you tell it to on your tablet or your heating that comes on when you swipe on your smart watch. The Internet of Things (IoT) is designed to make life easier, but it also opens up your home network to potential cyber-attacks. It doesn't mean you can't enjoy the benefits, but it does mean being aware of the potential negatives.

3 CHECK ENCRYPTION SETTINGS

Whenever data is sent over the Internet, it is 'encrypted'. This makes it harder to read if it's intercepted. You should look to use a strong encryption setting, such as WPA2, rather than WPA or WEP. You can check your router manual on how to do this.

4 KEEP YOUR SOFTWARE UP TO DATE

Manufacturers constantly update and improve software used in smart devices. Some will automatically alert you to an update, but not all do. To be on the safe side, it's a good idea to set reminders in your calendar. Check the manufacturer's website for any updates and run them if necessary.

5 RENAME THE 'GATEWAY' TO YOUR HOME

Your Internet router is the virtual gateway to your home network. It needs protecting. To do this, you should change the default name (the SSID) and password. You can usually find steps to do this in the instruction manual. Don't use your family name. Choose something more obscure. Make the password complicated too, using upper and lower-case letters, numbers and symbols. Do this for your router and any other smart devices connected to the Internet.

12 Top Tips To Get Smart About The DEVICES In Your Home

National Online Safety®

6 USE A SEPARATE NETWORK FOR GUESTS

If your router has a feature that allows you to set up a separate network for guests, you should use it. That way, when guests use your Wi-Fi, they won't have access to your devices.

7 SAY GOODBYE TO SIRI AND ALEXA

It's a good idea to change the activation words on your smart devices so they are unique to you and your family. This makes it that much harder for people to break into your smart devices.

8 DEACTIVATE ANY UNNECESSARY FEATURES

Though it's a fun idea, you probably don't need to control your kettle from outside the house. In fact, there are often many unnecessary features included on smart devices. Where possible, you should look to disable these. Doing so reduces the ability for people to hack your devices. When someone sees you've actively taken steps to increase security, they're less inclined to try to compromise them.

9 TRUST YOUR INSTINCTS

If you ever feel something is wrong or your network is being exploited, visit the manufacturer's website or ring their technical support department. It's better to be safe than sorry.

10 BUILD A WALL

You could also purchase a dedicated 'firewall' device. This is something that plugs into your network and stops cyber threats reaching your router. Some routers do have a firewall element included, but they are no replacement for the real thing. A firewall device thoroughly analyses information coming in and out of your network and helps stop malicious attacks. A security device is strongly recommended to anyone who works from home or deals with sensitive information.

11 SECURE YOUR SMARTPHONE

If you do use apps on your smartphone to control devices in your home, make sure your smartphone is secure. At the very least makes sure the pin function is enabled, as well as any biometric authentication you have. Where possible, it's also a good idea to download some anti-virus software for your smartphone too.

12 REGULARLY AUDIT YOUR DEVICES AND CONSOLES

Every now and then you should check through all of your smart devices (including games consoles connected to the Internet). Turn them off at the mains and disconnect them from the Internet. In fact, it's good practice to disconnect any devices that aren't in use. It's a small thing but really does help. Even when you think a device might be in sleep mode, if it's connected to the Internet it could still be listening or streaming data.

Meet our expert

Emma was a secondary school Computer Science teacher for more than decade. Since leaving education, she has been working in a cyber security firm delivering cyber awareness training to businesses and carrying out network testing. She is a mother of a five-year-old and has vast experience of controlling and managing how children access online services and use apps.

SOURCES: https://www.ncsc.gov.uk https://www.getsafeonline.org