

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.



Yorkshire & Humber
REGIONAL ORGANISED CRIME UNIT



National
Online
Safety®

#WakeUpWednesday

part of our Online Information Series



What you need to know about ...

FAKE NEWS



est. 2017

FREE - TODAY ONLY

Brought to you by



WHAT IS FAKE NEWS

Parven Kaur, Kids N Clicks Founder

Fake news can be false information, photos or videos purposefully created to confuse or misinform. It can also be genuine information that has been manipulated to deceive. It is important that children learn how to distinguish between real news and fake news, so that they don't inadvertently share something which isn't true or believe something which could be misleading.



For details, see page 13 ...



KNOW THE RISKS

SHOCK VALUE

Fake news can cause upset or shock to readers or viewers. Many fake news stories are written with appealing headlines and have content designed to create 'shock value', so the news spreads rapidly (common examples include the 'death' of a celebrity, company giveaways, news relating to supernatural events, or terror-related posts that provoke reactions).

EMBARRASSMENT

Fake news is often deliberately created to misinform people - whether for fun, out of malice or to support an ideological or political agenda. As it's often difficult to tell the difference, young people can easily believe what they see and then share something which is a hoax or a joke, leading to embarrassment or ridicule.

INFLUENCE BEHAVIOUR

Ultimately, fake news is designed to shape people's beliefs, thoughts and decisions: influencing them into believing something which has been misreported or which simply isn't true. This can shape how children think, behave or act in real life. It can especially affect their trust in the media or even in democracy itself.

FURTHER SUPPORT

REPORT THE CONTENT

Google and many social media platforms now have dedicated methods for fake news stories to be reported to them. This can range from sending a feedback message to Google via the page itself to the 'Report Post' buttons on Facebook and Twitter.

PROVIDE REASSURANCE

If your child feels as though they have been negatively impacted by a fake news story, or has suffered some form of embarrassment because of fake news, it's important to be supportive and reassuring. Discuss with them how not everything that's posted online is true.

IMPROVE THEIR DIGITAL LITERACY

If your child has been tricked by a fake news story, try to encourage them to think more rationally about what they see and hear on the internet. Advise them to question the motivation behind a story - such as why it's been written, and if it's trying to make them form a specific opinion or influence their actions.



HOROSCOPES
New to page 18 ...
Find out what's in your future!

SPOT THE SIGNS

CONSIDER THE SOURCE

Fake news stories can sometimes be identified simply because they are too ridiculous or outrageous to believe. Make sure that the website that published the story is a credible source, like a major news network or local paper which has the resources to fact-check published stories.

CHECK THE URL

Does the website address at the top of the page look real? An easy way to spot suspect stories is if they're located on a news site with an odd domain name. So check the URL. Some shady websites try to incorporate a legitimate news source into their URL (such as www.therealbbc.co.uk) or will slightly misspell a popular domain name.

VERIFY FACTS AND IMAGES

Authentic news is usually backed up by official data or surveys and previous, similar instances of the occurrence being reported. Similarly, fake news stories often include photos which have been manipulated. Perform a Google reverse image search to see if the picture has been stolen from another source and doctored.

RESEARCH THE WEBSITE

Be wary when a big story comes from a news organisation that you've never heard of. Some hoaxers will quickly set up a website just to spread fake stories and so-called 'breaking news'. Use the internet archive to research how long a site has been running - and check if the same story is being reported by more credible news outlets.

ARE ALIENS HARVESTING OUR WIFE?!



Supposed footage of alien craft.

Our groundbreaking exposé on page 4 ...

OUR EXPERT PARVEN KAUR



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.