HATTON ACADEMIES TRUST

Safer Internet Use

Tips for encouraging open discussion about digital life

Make your interest clear

Ask to see your child's favourite games and apps which will help you spot issues

Be open, honest, and appropriate to their age

When answering questions about puberty, relationships, etc.

Remind your child they can always talk to you

Even when they view harmful content, talking about it openly will help

Discuss that not everything we see online is real

Use examples from your own online world, like posts that show perfect houses

Try to remain calm

Your initial reaction could stop a child from speaking openly about what they've seen

Create a family agreement

About device use including when to use devices, parental controls and why it's good to talk

Keep talking

Online Safety Newsletter | February 2025

Safer Internet Day is 11th February!

The theme for this year's national Safer Internet Day is 'Too good to be true' and aims to raise awareness of online scams. Statistics show that 66% of 16-29-year-olds have fallen victim to a scam so this is far from a niche issue.

What are the risks?

Fraud

A scam is any dishonest scheme that tricks you into handing over your money and/or your personal details. As such it is a type of fraud. Scams affect people of all ages and with the rise of AI are becoming harder to spot.

Identity Theft

Some scams will ask you to fill in your personal details and may come from a trusted voice – pretending to be from a company that you know such as Royal Mail or Amazon. Scammers can then steal your personal details in order to e.g. take out credit cards in your name.

Financial Loss

Most scams are focused on relieving you from your money. Many of your children's phones, smart TVs and games consoles are linked to your bank accounts (e.g. via apps such as Amazon Prime) so even if your child doesn't have their own bank account they could fall victim to a scam that means that you suffer a financial loss. Goods should only be bought from a trusted website with a secure transaction option and financial details should never be given out by clicking on a link in a text or email – companies such as NatWest would never contact you asking you to share this information with them.

Staying safe online
Advice to share with your child

Tell a trusted adult if something upsets you

Take breaks from being online

Don't chat with strangers

Ask permission before downloading anything

Avoid sharing private photos

Don't give away personal information

Double check your news sources

Take notice of age restrictions

Stick to trusted apps

Be suspicious of new information

Show respect to others

Be honest with parents and carers

`

Examples of Scams

Scams include phishing (links in emails or texts that pretend to be from companies that you know), online shopping scams (selling fake or stolen goods or tickets or taking your money but giving you nothing in return), impersonation (something that pretends to be endorsed by a celebrity), romance scams (people pretending to have a romantic interest in you and then asking for money), and money muling (getting you to agree to them moving money through your accounts which will earn you a small percentage of the overall amount but will also earn you a criminal record)!

What to look out for?

Too Good To Be True?
If it sounds too good to be true it probably is! Does the price of the item look far too cheap? It is probably fake or non-existent. Your children may be buying you a gift and not know how much things should cost – talk to them regularly so that they understand the cost of things and that if something is too good to be true not to buy it.

False Urgency
If a company tells you that you must take action NOW (or within a very quick time scale) it is usually a scam tactic to stop you from pausing to think about what you are doing. Genuine companies will not pressure you into taking action immediately so this should tell you it is a scam.

Unexpected Contact
"I haven't ordered anything – why are DPD contacting me?" – Chances are they aren't and this is a scam message phishing for your details.

Asking for money or personal information:

- This is the main one – whatever the scam, whatever the tactics, sooner or later the person, message or interaction will ask you to share your personal details or payment details.
- Do not give out your details to anyone who you don't trust. Do not allow yourself to be rushed into making a quick decision. Once you have shared your information you are likely to lose money.

Starting a conversation about life online

Be positive and open-minded about the internet

Talk early and often
Make conversations about the internet part of your daily routine

Create a safe space for conversations
Talking face to face can sometimes be difficult, so talking while walking alongside or while in a car might be easier. Make sure there are no distractions

Keep it relevant
The way your child uses the internet will change as they grow older. So, ask open-ended questions to let your child lead the conversations you have to get a feel of the challenges and experiences they face online

Be proactive
Create an agreement together on how the internet will be used, including time spend online, who your child can communicate with, appropriate apps and games and safety tools to report and block harmful content

How can I keep myself safe?

- Secure websites usually start with https not just http. Look out for this before entering payment information on shopping sites.
- Some fake charities set themselves up to deprive well-meaning people of their hard-earned money. Check they exist on a website such as Charity Check before parting with your cash.
- Always download apps from your app store and not via links in other websites/social media sites.
- If unsure type the name of the website, or copy the message you have received, into a search engine such as Google along with the word 'scam'. A quick search will usually tell you if it's safe.
- If you think the message is genuine, contact the company back by using the contact details on their company website to check rather than clicking in the link or using the contact details that they have sent you.
- Talk it over with someone before acting and don't be pressured into making quick decisions.

What if I think I have been scammed?

- Call the Action Fraud line on 0300 123 2040
- Forward any suspicious text messages to 7726
- If you have given out any account details e.g. Amazon, log in to your account and change your password ASAP
- If you have given out payment details contact your bank/card provider to report this and ensure that the account/card is stopped and any fraudulent transactions are reported as such. The bank/card provider will then advise you on next steps.

How might this affect my child?

- Your child can easily have their personal details stolen (such as clicking on links to things such as personality quizzes on their social media sites that then collect these details when the quiz is filled out).
- Children increasingly have access to your financial information due to you saving payment details onto shared family computers or through the use of apps on smart TVs and game consoles that are linked to your bank accounts. Eventually they will have their own bank accounts and cards – starting conversations about this early saves issues down the line.
- Phishing scams don't know the age of the person they are contacting so your child is as likely to receive messages as you.
- Children with limited experience of relationships can be naïve about romance scams – encourage them to talk to you if anybody who they are speaking to online asks them for money.