MOUNT KELLY
Boarding and Day School
Boys and Girls, Aged 4-18

Safeguarding Bulletin

ISSUE 48

Mount Kelly's Safeguarding Bulletin aims to provide parents and carers with the information needed to have informed and age-appropriate conversations with their children about potential risks and issues in the wider world and online. This week's bulletin provides information about this year's Safer Internet Day theme: 'Too good to be true? Protecting yourself from scams online'.

Safer Internet Day is the UK's biggest celebration of online safety. Each year the initiative covers a different online issue or theme that speaks about the things young people are seeing and experiencing online. Created in consultation with young people across the UK, this year Safer Internet Day has focused on the issue of scams online and for young people, how to protect themselves and others, as well as what support is available to them. Follow this link for top tips for each age group.

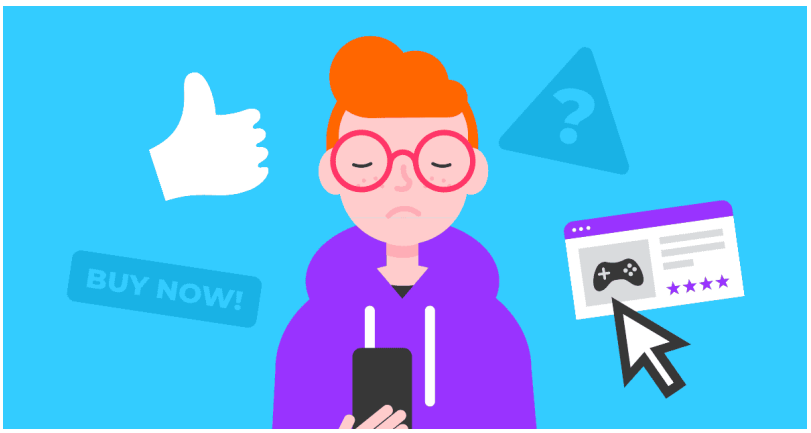
Scams and Fake News

While misinformation and 'fake news' are well-known concerns online, it's also the case that scammers and other cyber-criminals can try to utilise this phony material to manipulate, frighten or otherwise persuade their victims into cooperating.

With constantly evolving scams and such a high volume of misinformation online, it's vital that parents and educators know how to safeguard the children in their care against these kinds of tactics. The first of this week's guides breaks down the most prominent ways in which scammers attempt to use 'fake news' to their advantage, as well as how to protect youngsters from being manipulated by such techniques.

Social Media Scams

On any social media platform, you'll often come across links to genuine-looking websites. They might publicise 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, however, clicking on these links takes you to a fake website where you're asked to provide your personal details. In these instances, the whole enterprise is a ploy to capture sensitive information, such as your email address and password, which the scammers then exploit at your expense.



In the second guide, you'll find tips on helping young people to avoid potential risks such as phishing scams, untrustworthy URLs and 'payment first' scams.

At The National College, our WakeUpWednesday guides empower and equip parents, carers and educators with the confidence and practical skills to be able to have informed and age-appropriate conversations with children about online safety, mental health and wellbeing, and climate change. Formerly delivered by National Online Safety, these guides now address wider topics and themes. For further guides, hints and tips, please visit nationalcollege.com.

What Parents & Educators Need to Know about SCAMS AND FAKE NEWS

WHAT ARE THE RISKS?

"Fake news" refers to falsified or misleading material presented as a legitimate account of events. It's often used by malicious actors online to push an agenda, or even by criminals as a way of making scams more persuasive. Scammers can trick us into handing over personal information, security details and even our hard-earned cash.

"CLICKBAIT" PHISHING SCAMS

A message arrives saying "Have you seen this video of yourself?" or you might be sent an attention-grabbing headline about a celebrity that's been shared on social media. This kind of "bait" is produced by scammers to drive us to click on an unsafe link, where malware could be downloaded to our devices. These scams rely on our curiosity and our "need-to-know" instinct.

SALES, DEALS & DISCOUNTS

Some scams appear as adverts, offering a chance to buy something – such as designer products, expensive gadgets or tickets to a popular show – at a reduced price. Such ploys often include a time limit or countdown, urging us to hurry so we don't miss out on the deal. This pressure encourages us to input personal details or payment information before pausing to check if it's legitimate.

YOU'RE A WINNER!

This kind of scam involves fake giveaways, opportunities or freebies. It could be a message saying we've won a prize draw or competition. Or it could be a gift, free trial, bonus credit, and suchlike. It might claim that a package or refund is waiting. All these techniques are used to prompt us to share our personal information, thinking that there's something to be gained by doing so.

FALSE FRIENDSHIPS

Scammers often pretend to be someone they're not to gain their victims' trust. They might attempt to convince any children they connect with that they're a child of similar age with shared interests. Warning signs include a high volume of messages (often with an intense tone), secrecy, inappropriate levels of intimacy, guilt tripping, emotional manipulation, threats or blackmail.

PANIC MODE

To trigger a sense of panic, scammers may claim that a child's account has been hacked, or a virus has been installed on their device, or any number of other scary scenarios. They may claim to be able to fix the problem or offer a solution – if the child hands over control of the device or sensitive information. Similar scams involve impersonating a friend or relative, claiming that they're in trouble and need help.

FAKE CELEBRITY ENDORSEMENTS

Impersonating influential people online is a common tactic for scammers, who can use technology to create fake photos, audio and even videos that look authentic. These can be used to convince us, for example, to buy products, sign up for so-called "business opportunities" or invest in cryptocurrency schemes – all of which are fake or otherwise malicious. Many scams also involve the impersonation of popular companies' social media accounts, as well as those of individuals.

Advice for Parents & Educators

STAY INFORMED

Stay up to date with the latest information and best practice on cyber-security. See what scam stories are reported in the news and make note of what tactics were used. Keep up with young people's digital lives: talk about what they're doing online and use properly endorsed resources to learn what risks certain sites and apps pose to their younger users.

TALK TOGETHER

Chat often and openly with young people about fake news, online scams and how they both work. Encourage them to talk to you about anything they're unsure of or worried about online. If a child claims to have been scammed, don't pass judgement. Blaming the victim may deter young people from asking you for help. Remember: adults are scammed just as often, if not more.

ENCOURAGE HEALTHY SCEPTICISM

Most scams rely on emotional or psychological manipulation, tapping into our human instincts – whether that's to keep ourselves safe, help others, find answers, make friends, avoid losing out or to secure something we really want. Encourage children to recognise that pressure to act and to always consult with an adult – especially if what's on offer sounds too good to be true.

BE PROACTIVE

Children increasingly use digital devices for education, socialising, shopping and play. Don't wait for a problem to arise before you discuss the risk of scams, false information and fake news. Highlight what to look out for and clearly communicate under what circumstances the child ought to speak to an adult. Finally, ensure that they're aware of the support services that are available to them (such as Childline).

Meet Our Expert

Dr Holly Powell-Jones is the founder of Online Media Law UK and a leading expert in digital safety, media law and young people. Her PhD investigates children's understandings of risk online. She works with schools, businesses, and universities to provide award-winning education on the criminal, legal and ethical considerations for the digital age. Visit OnlineMediaLaw.co.uk for more.

#WakeUpWednesday®

The National College®

Source: See full reference list on guide page at: https://nationalcollege.com/guides/fake-news-and-scams

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 05.02.2025

At The National College, our WakeUpWednesday guides empower and equip parents, carers and educators with the confidence and practical skills to be able to have informed and age-appropriate conversations with children about online safety, mental health and wellbeing, and climate change. Formerly delivered by National Online Safety, these guides now address wider topics and themes. For further guides, hints and tips, please visit nationalcollege.com.

What Parents & Educators Need to Know about SOCIAL MEDIA SCAMS

On any social media platform, you'll often come across links to various websites. They might include exclusive online shopping offers or invites to complete a quiz and earn a particular reward. In some cases, however, these links lead to illegitimate sites or ask for personal details - a ploy to capture sensitive information, which scammers then exploit.

FAKE PHONE DEALS

Criminals will contact you pretending to be your mobile phone vendor offering an upgrade or discount on your contract. They will seek to gain personal data along with the username and password associated with your account, before then using this info to either take control of your phone number or order phones, devices or new contracts through your account, before selling these on.

ROMANCE SCAMS

Fake profiles are sometimes created on dating sites or social media to manipulate other users with the promise of romance. They might spend significant time gaining their target's trust in text chats, before encouraging them to send explicit photos with the promise of this being reciprocated. In many cases, these images are instead used for blackmail – most commonly demanding money to prevent the scammer from sending these intimate images to the victim's friends and family.

MALICIOUS APP DOWNLOADS

Some cyber-criminals design apps that appear genuine or helpful – and are normally free – but have instead been created to steal your personal information. For example, a pop-up could appear, warning that your device is infected with viruses and recommending you install their anti-virus app – which does nothing but grant cybercriminals access to your device and any information you have stored on it.

SOCIAL MEDIA IMPERSONATION

Another method employed by scammers is the creation of fake social media accounts to trick people into sharing personal information or sending money. They could impersonate an influencer, a money expert, or someone else trustworthy, and tempt users into sharing private information: asking for payment information to take part in a prize giveaway, for example. In these cases, the offer simply doesn't exist, and any information disclosed will end up in the scammers' hands.

FAKE EXAM PAPER SALES

Particularly during the exam period, criminals will use social media to advertise 'leaked exam papers' for sale to students who want to get an advantage. Unfortunately, these papers are often either outdated or completely fake. Whether the paper was authentic or not, many exam boards may consider any attempt to buy one an offence and could disqualify a student from all exams for this.

'PAYMENT FIRST' SCAMS

On platforms that let people sell goods, like Facebook Marketplace, a malicious user can list an item for sale, requesting payment up front. Most online stores work this way, but the crucial difference here is that scammers ask for payment through a channel which isn't regulated by the site itself – such as a direct PayPal transfer. If the user pays in this way, the scammer never sends the item, and the payment can't be reclaimed.

Advice for Parents & Educators

STICK TO REPUTABLE RETAILERS

Be wary of any offers which seem too good to be true or where the fear of missing out (FOMO) is emphasised: this could be criminals seeking to exploit human behavioural weaknesses. Where possible, use respected retailers and online vendors as their offers are likely to be more trustworthy. If something looks too good to be true, then it probably is.

BEWARE A SENSE OF URGENCY

Criminals often try to convey a sense of urgency to pressure users into acting without thinking. For example, a scammer pretending to be your bank may ask for your payment details to investigate 'fraudulent transactions' on your account. Proceed with care where such immediacy is emphasised; question *why* this person seems to be trying to make you panic.

INSTALL ANTI-VIRUS SOFTWARE

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

KEEP YOUR INFORMATION SECURE

Always ensure that your passwords aren't easy to guess; make them out of three random words, providing something long but memorable. Change your password if you have any concerns about your account's privacy, while enabling multi-factor authentication on all accounts to make unauthorised access more difficult. You should also avoid ever entering personal information on unfamiliar websites, as this could result in key information being passed on to a scammer.

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 and delete it. They could be a scammer who's seen your email address on your social media profile or had your contact details sold to them by a third party. The best defence you have against phishing attempts is to remain vigilant.

REVIEW PRIVACY SETTINGS

Regularly review your privacy settings on social media. You can restrict which parts of your profile can be seen and by whom. We recommended hiding your personal information from anyone except trusted friends and family, which significantly limits the details a scammer can use against you. It can also be safer to only accept friend or follow requests from people that you already know.

Meet Our Expert

Gary Henderson is the Director of IT at a large independent boarding school, as well as a member of the Digital Futures Group, Vice-Chair of the ISC Digital Advisory Group and an Association of Network Managers in Education Ambassador. Having worked in education for over 25 years, he's also a Certified Information Systems Security Professional and a Microsoft Innovative Educator Expert.

#WakeUpWednesday®

The National College®

Users of this guide do so at their own discretion. No liability is entered into. Release date: 15.09.2021 Last reviewed: 21.05.2024