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

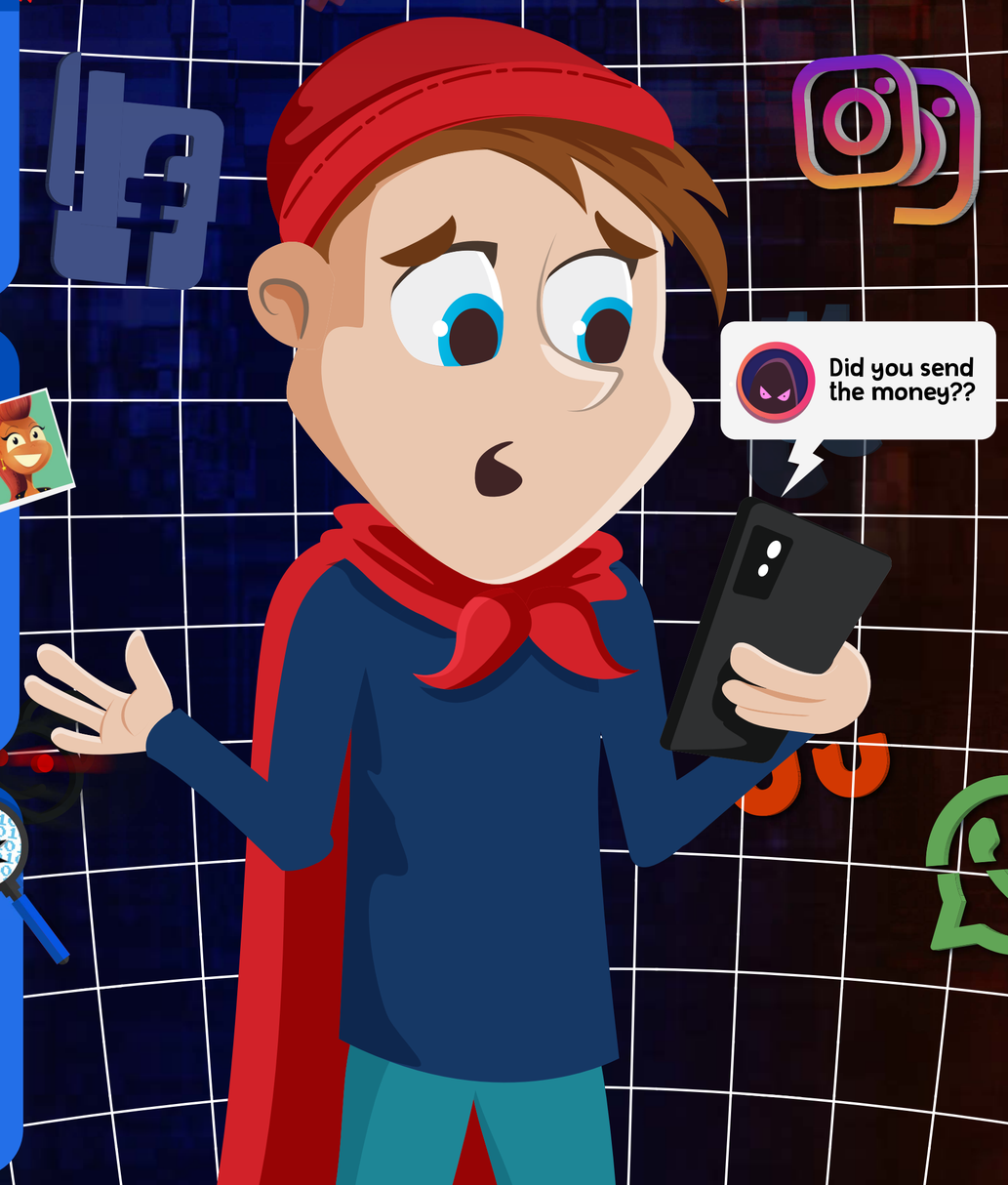
Criminals will contact you pretending to be your mobile phone vendor offering an upgrade or discount on your contract. They will seek to gain personal data along with the username and password associated with your account, before then using this info to either take control of your phone number or order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