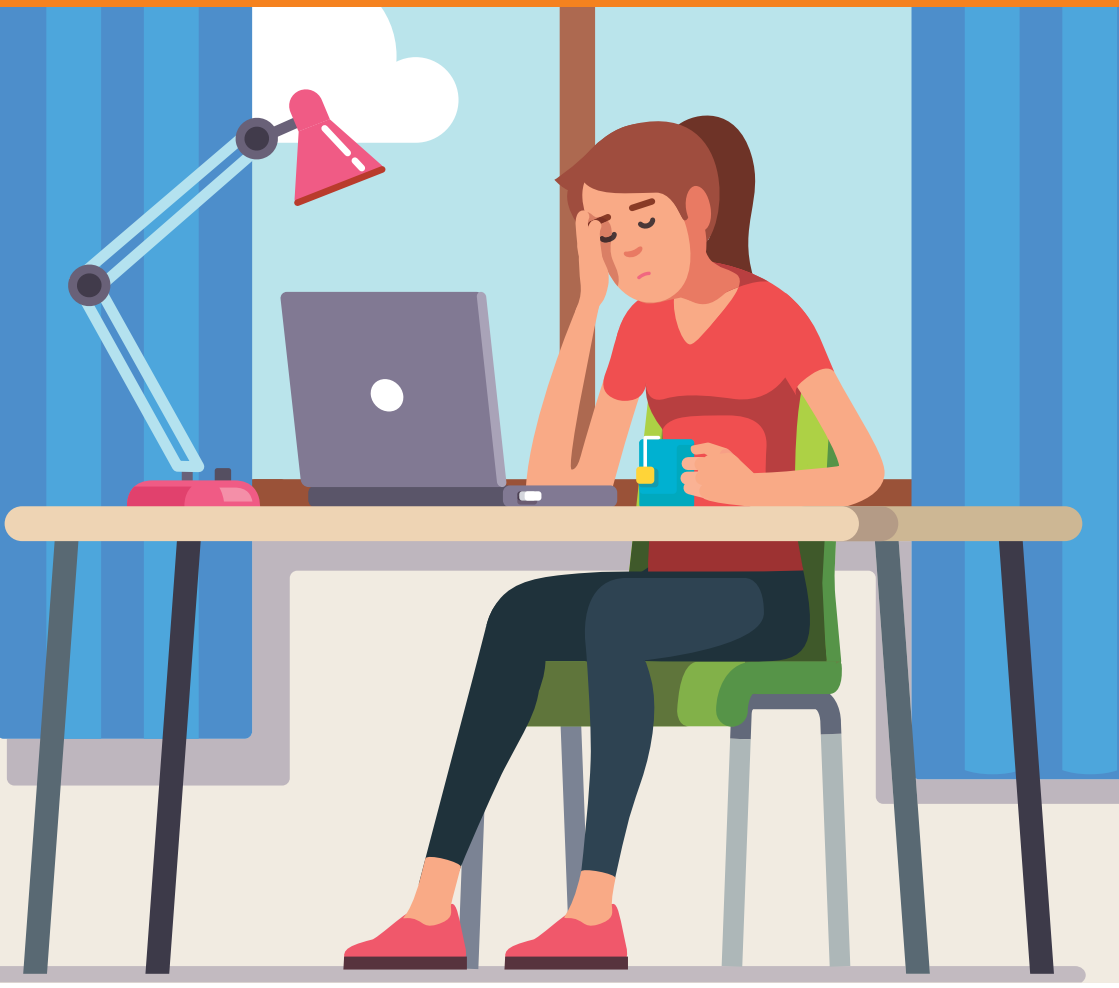
Did you know you can get scammed on social media?



GET SAFE ONLINE .org

NEIGHBOURHOOD WATCH

www.getsafeonline.org

You're probably familiar with some of the ways in which fraudsters approach and attempt to lure in their victims, such as emails, texts, phone calls, letters and traditional doorstep scams.

But did you know that social media is also a favourite place for scammers?
With billions of people using social media every day and the trust many place in the platform and fellow users, it shouldn't come as a surprise. Plus, at the moment, you have a lot on your mind, so it could be easy to drop your guard.

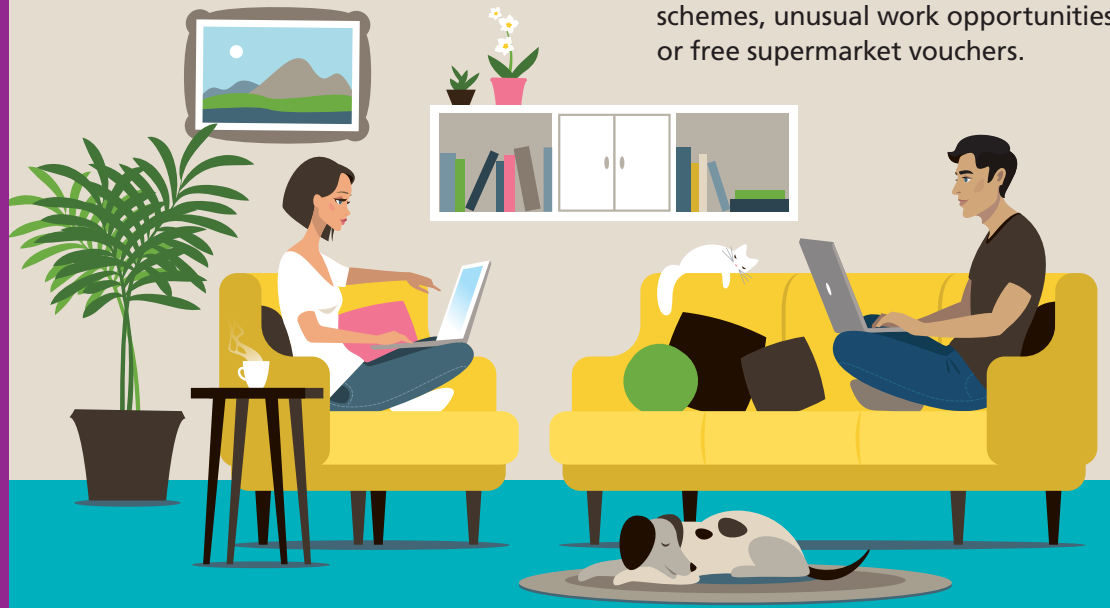
There are a number of ways that social media is used as a means to commit fraud. Examples include links in posts or DMs which advertise content, free items, special offers or quizzes, but which actually lead to fraudulent websites designed to steal your money, identity, or both. Posts instructing you to call or text a number, which turns out to be premium rate. And fake customer service Twitter accounts with fraudulent support links.

#socialscams

Top tips to avoid social media scams

Our online safety experts have put together some simple tips to help you avoid becoming a victim of social media scams.

- Don't click on **links in posts, tweets or direct messages** unless you're 100% certain that they're genuine and well-intentioned.
- Don't respond to posts offering **free app downloads**, as these may be fraudulent. Download apps only from the authorised app store for your device.
- Don't respond to **online quizzes or questionnaires**, however engaging they seem. The data you provide may be sold to third parties, and developers could obtain sensitive information from your profile, friends and IP address.
- Fraudsters frequently use social media platforms to advertise fake or non-existent goods. Do all you can to **check the authenticity of the seller** and **never pay by bank transfer** in case it's a fraud.
- **Don't click on shortened URLs (website addresses) or QR** codes, as they may divert you to a fraudulent website.
- Think twice before responding to approaches such as **friend/contact requests** or approaches to take some **unusual or irregular action**.
- Learn to recognise **fake notifications or warnings of financial problems, or offers that seem too good to be true**. These could include investment opportunities, get rich quick schemes, unusual work opportunities or free supermarket vouchers.
- Check that any communications via Twitter feature the **correct handle of the authentic organisation**. Even if they appear to have come from an organisation you trust, their account may have been hacked or spoofed.
- If in doubt, **call the correct number of the organisation or individual** who the post or tweet claims to be from, to check its authenticity.
- **Ask yourself** if a genuine organisation or individual would really contact you in the way they have.
- **Get into good basic habits** like using strong, unique passwords for social media accounts, not sharing personal information, making your accounts private, having up-to-date information security software/app and not using public Wi-Fi when what you're doing is confidential.

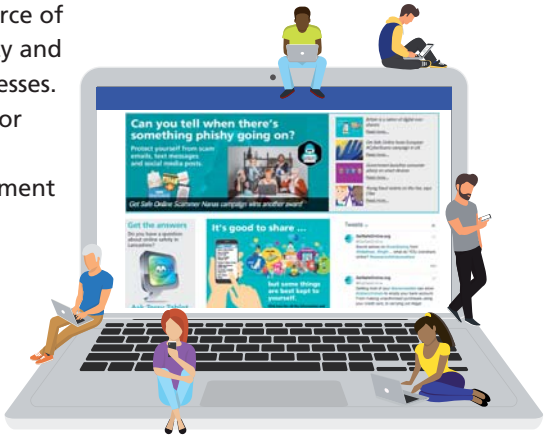


If you become a victim of a social media scam

- Report it to the social media network via the reporting mechanism on the site or app
- If you have lost money as a result of social media scams or via any other fraudulent activity, report it to Action Fraud, the UK's national fraud reporting centre by calling **0300 123 20 40** or by visiting **www.actionfraud.police.uk**

Get Safe Online

Get Safe Online is the UK's leading source of information and advice on online safety and security, for the public and small businesses. It is a not-for-profit, public/private sector partnership backed by a number of government departments, law enforcement agencies and leading organisations in internet security, banking and retail.



For more information and expert, easy-to-follow, impartial advice on safeguarding yourself, your family, finances, devices and workplace, visit **www.getsafeonline.org**

If you think you have been a victim of fraud, report it to Action Fraud at actionfraud.police.uk or by calling 0300 123 2040. If you are in Scotland, contact Police Scotland on 101.

GET SAFE ONLINE .org

NEIGHBOURHOOD WATCH

www.getsafeonline.org

OFFICIAL PARTNERS

TESCO · NatWest · Gumtree · Standard Life · first direct · PayPal · HSBC · Royal Bank of Scotland · M&S BANK · LLOYDS BANK · HALIFAX · BANK OF SCOTLAND · creativevirtual · ROYAL AIR FORCE · HM Government · CITY OF LONDON POLICE · NPCC · NATIONAL TRADING STANDARDS eCrime Team · cifas · VICTIM SUPPORT · EUROPOL EC3 · NCA · ActionFraud · METROPOLITAN POLICE · Ofcom · neighbourhood ALERT