12 Scams of Christmas

1 - Subscription trap; This scam offers a gift or trial offer. If you pay postage and packaging to receive the 'gift' you may, without realising it, set up a Continuous Payment Authority (CPA) allowing the company to take any amount out of your bank account at any time. You should report these to Citizens Advice.

2 – Bogus charities; Fake charities prey on the victim's sense of good will at this time of the year, and their marketing techniques can be very convincing. Make sure that the marketing you have received is genuine. If you aren't sure – don't take the risk. You can check if a charity is genuine by visiting the gov.uk website.

3 – Fake online shops; Criminals create fake websites which look reliable and offer all kinds of products from jewellery to clothes, technology and more at cheap prices. Don't be attracted by these low prices as after sending the payment, you may not receive the product! Check if the website you order your Christmas presents from is legitimate by visiting scamadvisor.com.

4 – HM Revenue & Customs; Criminals phone unsuspecting members of the public and claim they have over/under paid their tax. Beware - *never* give out your bank details, hang up the phone immediately and report to Action Fraud

5 – Bank scams; Criminals may phone you and claim to be calling from your bank to report 'suspicious activity' on your account. If you receive a call like this, hang up immediately and phone your bank on a number you know to be legitimate (e.g. from the bank's website)

6 - Purchase scams; you may be tricked into sending money via bank transfer to buy goods or services, often advertised online, which do not actually exist. When you shop online this Christmas, the best ways to keep safe are to buy from a trusted retailer whenever possible, and always pay by card for the greatest protection.

7 - E-greeting (online) cards; Be careful when sending/receiving online greeting cards as they can contain malware which can find address books and bank details stored on your computer.

8 – Bogus gift cards; Gift cards are ideal for that 'hard to buy for' person, but be aware if you are buying these online, as gift cards are easy to illegitimately replicate and could cause embarrassment to your friends and family when they try and use your gift… and they are fake.

9 – Delivery scams; Deliveries will inevitably increase this time of year as presents are bought so it's hard to keep track. Criminals use this as an opportunity to target consumers. If you get a text saying that your package requires payment for it to be delivered, it's probably a scam! Report it by forwarding the message for free to 7726 (spells 'SPAM' on your telephone keypad).

10 – 'Brushing' scams; the sellers on Amazon Marketplace may send you unsolicited parcels to create fake increases in their sales numbers. Amazon sellers are banned from sending such parcels by the company so if you have received one, make sure you report it to the Amazon customer service team.

11 – NHS Covid Pass scams; Messages saying you're eligible to apply for a Covid Pass are sent via texts and emails claiming to be from the NHS. They include a link the appears to be to the genuine website but is in fact a scam website set up to steal your personal details. Vaccine passes are completely **free** via the NHS app or by asking a physical pass to be posted to you.

12 – Extortion scams; Criminals contact you claiming they have embarrassing or incriminating information about you and threaten to release that information if you don't send them payment. If the criminal shows you they have a password you're currently using, change that password immediately. Remember, these scam messages are designed to scare you, don't fall for it!