The 12 scams of Christmas

'Tis the season to be cautious

1 Refund Scams

You may receive an email or text pretending to be from the Council or a well-known store promising a credit or tax refund and a link to click to claim the money back. They'll ask for bank details. DON'T

2 Look-a-like websites

This year, more than any, we are buying presents online. Criminals have set up fake websites that look identical to steal personal details and money. Secure website addresses start with 'HTTPS' and display a padlock.

3 Phishing Emails

Criminals send emails that look genuine to make you click on a link to a fake site or open an attachment that infects your machine with a virus. They will make you panic and rush your decision. THINK before clicking.

4 Phone Scams

Criminals ring you to discuss a topic then ask you to press a number on your phone keypad to "opt out" of a survey for example. It will generate extreme charges which the criminals will profit from. DON'T

5 Gift Card Scams

Received an email from a friend asking to buy gift cards for them? Criminals clone and pretend to be people you know to get you to do this. They are after the code on the card to spend the money. DON'T

6 Cost of Living

A message from a loved one claiming they have changed their phone number. A short while later, they ask for money. They may give a variety of reasons, but they often say the money is to help solve 'a problem which needs payment'. Known as a 'Friend in Need' or 'Mum and Dad' scam and more people than ever fall for it due to the cost of living crisis.

7 Fake delivery notifications

Over December you'll have packages being delivered on a daily basis. Criminals are cashing in on this and sending chance phishing emails disguised as well-known couriers hoping to get you to log in and share your details. If you are ever in doubt ignore the email and login/ get in contact via the companies official secure website.

8 Energy Scams

Refund scams from energy companies either via email, text or letter entice you by offering money back when really, they are scammers asking you for your personal data. Always be sceptical and reach out to your energy provider directly via their official communication channels.

9 Fake Charities

Watch out for criminals using legitimate charity names to appeal for a donation. Ask to see their official charity ID which they are required to carry. Trust your instinct.

10 E-card Scams

Watch for those e-cards you receive online. It could be infected with a virus that could shut down your device and you could be held to ransom to restore files. Get an Anti-virus installed that will alert you!

11 Fake Romance

Looking for festive love online? Criminals are too... The relationship develops over time and the individual is convinced to make payments to the criminal - DON'T. They're also after your identity. Guard your privacy.

12 Shopping Scams

Love top brands with low prices? Well stay vigilant for counterfeit goods. These range from poorly made clothes to dangerous electronics which fail to comply with safety laws. If it sounds too good to be true, it probably is.

If you are a victim of a scam, report it to Action Fraud via www.actionfraud.police.uk
If you are a business, charity or organisation which is suffering a live cyber-attack, call Action Fraud - 0300 123 2040
To find out more advice and guidance on cyber security, visit the National Cyber Security Centre (NCSC) at https://www.ncsc.gov.uk