Cyber & Digital Crime Unit
Email: cyber@cumbria.police.uk

Chief Constable
Chief Constable Robert Carden
Police Headquarters
Carleton Hall Penrith,
Cumbria
CA10 2AU

www.cumbria.police.uk

SHOPPING ONLINE - FESTIVE SEASON

Delivery Fraud. As people shop online over the festive period, there will be huge numbers of parcels being delivered across the country, which criminals may look to take advantage of.

Criminals contact you hoping you are waiting for a parcel to arrive. They want access to your money and information or for you to click on links which could download malware to your device.

Instead of clicking the link, log into your account directly to update or check your information.

How to protect yourself:

• Remember that criminals will send out texts, emails and other messages with links leading to fake websites used to steal personal and financial information. These messages may appear to be from trusted organisations and may use official branding to convince you they're genuine.

• Always access websites by typing them into the web browser and avoid clicking on links in texts.

• Remain vigilant and check delivery notifications very carefully to ensure they are genuine. Check what you've ordered online and track your parcel through the websites of legitimate delivery companies.

• Always question claims that you are due goods or services that you haven't ordered or are unaware of, especially if you have to pay any fees upfront.

• Customers can report suspected scam texts to their mobile network provider by forwarding them to 7726.

Impersonation Scams. This is where you're convinced to make a payment or give personal and financial details to someone claiming to be from a trusted organisation such as your bank, the police, a delivery or utility company, communication service provider, a government department such as HMRC or someone you trust such as a friend or family member.

Criminals will take advantage and attempt to impersonate trusted websites and organisations. They'll use the same pictures as other websites for products with 'too good to be true' offers.

Over £22m was stolen through impersonation fraud in the first half of 2024.

How to protect yourself:

- If the offer is too good to be true, ask yourself why.
- Research the company or person you're purchasing from and read reviews.
- Make sure you're on a genuine seller's website by checking the website link and avoid clicking on links from social media, message or email.
- Only criminals will try to rush or panic you.

Purchase Fraud. This happens when criminals trick you in to paying for goods or services that don't exist. This can be from online auction sites or via social media.

Criminals also use cloned websites with slight changes to the URL to trick you into thinking you're purchasing from the genuine site. They may also ask for payment prior to delivery and send you fake receipts and invoices that appear to be from the payment provider.

As we approach the festive period it's important to keep your guard up when buying things online.

A total of £42.3 million was lost to purchase fraud in the first half of 2024. Losses are now at their highest point since 2020.

How to protect yourself:

- Be cautious of any "too good to be true" offers.
- Research the company or person you're purchasing from and read reviews.
- Make sure you're on a genuine seller's website by checking the website link and avoid clicking on links from social media, message or email.
- Run a reverse image search on Google to see if photos are being used in multiple places.
- Always use a secure payment platform from trusted retailers – avoid paying with bank transfer. Where possible, use a credit card when making purchases over £100 and up to £30,000.
- You can search for the company's details on GOV.UK. This will tell you if where you're purchasing from is a registered company or not.
- Only criminals will try to rush or panic you.

Take Five and stay safe!

ActionFraud
National Fraud & Cyber Crime Reporting Centre
actionfraud.police.uk