Fraud Counts Newsletter

December 2023

WELCOME TO THE CHRISTMAS EDITION OF THE FRAUD COUNTS NEWSLETTER



The Christmas period should be, and normally is, a time to get together with friends and relatives.

Christmas means many different things to different people, but whatever someone's background and beliefs, it should be a period when you can unwind, relax and enjoy yourself.

Whilst, for most people, most of the time, this is very much the case, Christmas can also be a time of rich pickings for fraudsters.

We wish all our readers a Merry Christmas and hope this newsletter helps you to stay safe from scammers and enjoy the festivities.

Scam alert: UK Finance warns public to beware of parcel delivery scams in the run up to Christmas

UK Finance is warning consumers to be vigilant against criminals looking to defraud them by posing as parcel delivery companies, as more people across the country are expected to shop online this Christmas than ever before.



This Photo by Unknown Author is licensed under CC BY

Intelligence from UK Finance suggests that criminals are sending out phishing emails, purportedly from well-known delivery companies, which claim that they have been unable to deliver parcels, packages or large letters. These emails may ask the recipient to pay a fee or provide additional details in order to arrange the delivery.

The public should also be aware of an increased risk of scam phone calls and texts impersonating delivery companies, as well as fake delivery notices posted through letterboxes. Similarly, these will ask for advance payment or for customers to provide information that is later used to defraud them.

Customers are typically tricked into clicking on links to seemingly genuine websites requesting personal and financial information such as their address, date of birth, mobile number or bank details, which are then used to commit fraud. In some cases, victims later receive a call from the criminal pretending to be from their bank 's fraud team, trying to persuade them to move their money to a safe account or reveal their pass codes.

Take Five to stop fraud



Fraud poses a major threat to the UK. It's a crime that the finance industry is committed to tackling, but it's also one that requires the combined efforts of every sector, both public and private, to overcome.

Take Five is a national campaign that offers straight forward and impartial advice to help everyone protect themselves from financial fraud. This includes email deception and phone-based scams, as well as online fraud – particularly where criminals impersonate trusted organisations.

Visit Take Five's website for further information - **https://www.takefive-stopfraud.org.uk/**

Christmas trees being offered as investment

Investments in Christmas trees have previously been unheard of, but the National Fraud Intelligence Bureau (NFIB) has received reports that suggest Christmas trees are being offered as a commodity for investment. Whilst we cannot comment on viability of investment in Christmas trees, it is of concern due to this being promoted by applying the same tactics that we have seen in investment fraud; cold calling, high pressure sales, promise of high returns etc.

Follow our advice to avoid falling victim to investment fraud:

	If you get a call out of the blue, be wary. If in doubt, don't be polite, just hang up.
	If you're considering any type of investment, always remember, if it seems too good to be true, then it probably is. High returns can only be achieved with high risk.
	Never be rushed into an offer and always be on your guard against anyone trying to push you into a deal.
	Take the time to seek independent legal or financial advice before deciding.
	Always check the credentials of the company you're dealing with. Check for known fraudulent organisations at the Financial Conduct Authority (FCA).

If you receive one of these investment cold calls, ignore it and report it to Action Fraud **- https://www.actionfraud.police.uk/**

©ASW Assurance

The top five worst scams of Christmas 2023

1. Lookalike shopping websites

Online shopping scams can take place at any time of the year but are especially prevalent during the holiday shopping season.

Fraudsters create fake, spoofed and lookalike websites with too good to be true deals on popular items, in order to trick their victims into sending payments or sharing their credit card details and personal information. At best you may receive a counterfeit item, at worst scammers could steal your identity and wrack up debt on your credit card, or even open a new account in your name and drown you in debt.

Fake shopping sites will often ask for payments in gifts cards, wire transfers, cryptocurrencies or even using payment apps like 'Venmo' or 'cash app'.

How to avoid fake online stores this Christmas season:

- Only shop from online retailers you know and trust. You're less likely to get scammed when shopping on the shop's office website.
- Double check the URL and site details before entering information. Lookalike holiday scams may also use professional web designs to closely mirror the appearance and feel of a standard retailer's site, but are often riddled with errors like typos, suspicious URLs, or incorrect customer service phone numbers.
- Use safe browsing tools to warn you before it's too late.

2. Fake social media ads for the holiday's hottest gifts

According to one study, 40% of all online shopping scams come from Facebook and Instagram ads. Scammers may use hacked accounts and stolen photos to advertise steep discounts on luxury or in demand goods, but the products either don't arrive, or are cheap knockoffs of what was advertised.

In an even more recent scam, fraudsters use TikTok and other social media platforms to pose as disgruntled employees who are 'exposing' steep discounts from their previous employer, as long as you're willing to pay steep shopping costs upfront.

How to avoid social media scams over the holiday season:

- Don't believe too good to be true deals. Fraudsters use steep discounts to get you to ignore the red flags of their scam. If a deal seems too good to be true then it most likely is.
- Research who posted the ad. Don't blindly trust ads on social media. Check the official page that posted the post to see if it is legitimate.
- Always check where a link is taking you. Hoover over links on desktops computers to see where they're taking you before clicking.

©ASW Assurance

3. The puppy scam

Every Christmas, thousands of children get new puppies. As if, on cue, puppy scammers impersonate breeders and post fake litters for sale. Social media ads offering puppies for sale at a discounted price are an immediate red flag. Many phony sellers also ask for the money upfront to cover the cost of shipping, insurance, and vaccinations. In one example, a woman was tricked into sending $400 to an online breeder via Western Union. But once the transfer was accepted, the breeder's website disappeared and she never heard from them again.

If you're buying a puppy or a pet for your family this Christmas, work with a local breeder who you can meet in person. Or, even better, visit your local rescue centre.

4. Spoofed delivery notification texts and emails

With so many people shopping online, fraudsters send fake delivery notifications claiming your packages are delayed, require payments, or have other issues that need your attention. These emails and text message scams will include a link to click to ''solve'' the issue. But, if you click it, you'll be taken to a fake website that will steal your personal and payment information.

How to avoid fake delivery notifications this Christmas:

- Block spam text messages on your phone. Most smartphones allow you to block texts from unknown senders
- Don't click on links in suspicious messages. Any unsolicited text messages or emails are a potential phishing attack. Be very careful before clicking on the links in them.
- Check your delivery status directly with the shipper/supplier. Instead of clicking on links in a message, go to the shipper's official website and enter your tracking number to see if there is actually an issue.

5. Fake job postings for temporary holiday jobs

Scammers know that the Christmas holidays can be financially hard on many people. Fraudsters post bogus 'work from home' or in person temporary holiday jobs to trick jobseekers into sharing their personal information or paying for non-existent 'training' materials. In one scam, an ad for airport shuttle drivers was posted on a 5000 member Facebook group. Those who started the application process quickly got suspicious when they were asked to supply sensitive information such as copies of their driver's licence and bank details.

How to avoid fake job scams over the holiday season:

- Don't share sensitive information in a job application. Wait until you've been hired and are sure the opportunity is legit before sharing your bank details and other sensitive information.
- Question the interview process. Job scams will have short interviews, often over messaging platforms like WhatsApp. If you never speak with an actual recruiter or manager, it could be scam.
- Do your own research on the company. See if they have an online presence and reviews on a third-party site like the Trading Standards or Trustpilot.

©ASW Assurance

Just for fun, try our Christmas song quiz!



♪ *Frosty the snowman was a jolly happy soul* ♪ and bought tickets to see a pantomime from a dodgy website. Do you think Frosty received the tickets they paid for?

YES **NO**

One of the elves received an email saying ♪ *All I want for Christmas is you* ♪. The email contained a link to an e-card from the Grinch and downloaded a virus. Can you be sure to trust e-cards?

YES **NO**

On a ♪ *silent night* ♪ the Three Kings with arms full of presents left the door on the latch so anybody could come in. Did they do well?

YES **NO**

The Deputy Chief Elf ♪ *wished it could be Christmas everyday* ♪ when they bought a new sleigh from an auction site but paid by money transfer rather than going through the auction site. Do you think they ever got their sleigh?

YES **NO**

Santa Claus was ♪ *driving home for Christmas* ♪ and pulled into a service station to grab some food for the car journey. Santa left their Christmas shopping in view on the back seat of the car. Did Santa do well?

YES **NO**

Rudolf was ♪ *dreaming of a white Christmas, just like the ones they used to know* ♪ when they authorised payments of agency staff invoices despite the authorising signatures not matching the specimen signature list. Do you think Rudolph got defrauded?

YES **NO**

©ASW Assurance

Our Local Counter Fraud Team

Our Local Counter Fraud Specialists are fully accredited with the University of Portsmouth. We aim to prevent and deter fraud and hold those to account who commit fraud against the NHS.

Counter Fraud Services are provided by ASW Assurance (www.aswassurance.co.uk), an NHS consortium providing counter fraud and internal audit services to NHS and healthcare organisations.

If you would like to know more about our Counter Fraud work or arrange for your department to receive a Fraud Awareness Presentation, please contact your Local Counter Fraud Specialist (LCFS) below.



Gareth Cottrell – Counter Fraud Manager

✉ gareth.cottrell@nhs.net ☎ 01872 258057
07814 002364



Tracy Wheeler – LCFS

✉ tracy.wheeler2@nhs.net ☎ 01752 431378
07789 868568



Byron Kevern – LCFS

✉ byron.kevern@nhs.net ☎ 07775 417508



Sarah Smith – LCFS

✉ Sarah.Smith10@uhbw.nhs.uk ☎ 07467 685609



Sandra Bell – LCFS

✉ sandra.bell19@nhs.net ☎ 07467 685529



Ian Halkerd – LCFS

✉ ian.halkerd@uhbw.nhs.uk ☎ 07788 300215



Sammy Donaldson – Trainee LCFS

✉ s.donaldson1@nhs.net ☎ 07467 685529

©ASW Assurance