DECEMBER 2024

AUDIT YORKSHIRE

COUNTER FRAUD NEWSLETTER

The Counter Fraud Team would like to wish you all a very happy, fraud-free festive period!

You better watch out...

Whatever this time of year means to you, it's important to be aware that it's a prime time for fraudsters to strike. The period between November and January covers some major online shopping events such as Black Friday and the January sales. It's also a time of year when you might be thinking about donating to charity, welcoming a new furry friend, or planning getaways for 2025.

As fraud is the most common offence in England and Wales, it's important to stay vigilant, refresh your awareness, and know how to get help and advice.

Throughout this newsletter, we'll look at some of the scams that are more common at this time of year. Our new colleague, Rudolph the Red Flag Reindeer will offer some advice along the way to help you to keep yourself and others safe. As ever, if you have any questions or concerns, please don't hesitate to reach out to your Local Counter Fraud Specialist.

Parcel Delivery Scams

With so many people shopping online or receiving gifts through the post, fraudsters seize the opportunity to carry out parcel delivery scams. These come in several different forms - you might get an email, text or phone call at the start of this scam.

The person contacting you will impersonate a known delivery company and will claim that there's an issue with your delivery. They might claim that there has been a problem finding your address, that the sender didn't pay enough postage, or that your delivery has had to be rescheduled.

If contacted by email or text you'll be invited to click on a link to sort out the issue. You will then be asked to "confirm" your name and address and will be prompted to enter payment details, often for a small fee of £2-5.

If the fraudster has contacted you by phone they will ask for these details over the phone or may ask if they can email or text you with a link to follow.

Once the fraudster has got hold of this information, the second part of the scam will start. You'll get a phone call from someone claiming to be from your bank's fraud team. They'll explain that they've got some concerns that you might have been scammed, and then try to persuade you to transfer your money into a "safe account".

Rudolph the Red Flag Reindeer's Advice

If you are contacted about a delivery and you are expecting a parcel, get in touch with the company you placed the order with or use the tracking information they have provided to you to check on the status of your delivery.

Be very cautious about links in emails and text messages.

Beware of spoofing. Fraudsters can alter how they appear when they send you texts or call you over the phone - disguising their phone number with the name of a trusted company or the actual phone number used by your bank's fraud team.

If in doubt about a phone call claiming to be from your bank, hang up. Wait 15 minutes or use a different phone to call the number on the back of your bank card.

Puppy Scams - Don't bark up the wrong Christmas tree

Puppy scams are designed by fraudsters who advertise puppies for sale, usually through online platforms like social media, classified ad websites, and even specialised pet sale websites.

How the scam works:

The advert: Scammers post photos of adorable puppies, sometimes using stolen images from legitimate breeders' websites. These listings usually showcase desirable or rare breeds at very attractive prices, designed to lure in prospective buyers.

Initial Contact: When a person expresses interest, the scammer quickly responds to establish rapport and urgency. They may claim the puppies are in high demand or that the buyer needs to act fast to secure the dog. They may also try to move the conversation off the app or website, and onto an alternative platform such as WhatsApp. That way, if someone else reports their profile, they don't lose other potential victims.

Payment Requests: The scammer asks for payment upfront, often through non-traceable methods like bank transfers, gift cards, or mobile payment apps. Some may even go as far as setting up fake third-party payment websites to add a layer of legitimacy.

Additional "Fees": After the initial payment, scammers may request additional payments citing, insurance fees, Kennel Club registration, microchipping or vet bills. These fees may continue to pile up, with the scammer reassuring the buyer each time that they're just one step away from receiving their puppy.

The Disappearance: Once the victim stops making payments or starts to ask too many questions, the scammer vanishes. At this point, the buyer is left without their money and, heartbreakingly, without a puppy. In some cases, the fraudster arranges for the person to collect their puppy, but sends them to a random address and deletes their profile / adverts.

Warning Signs of a Puppy Scam:

Unusually Low Prices: Scammers often lure victims in with low prices compared to the typical costs for that breed.

Limited Information: Vague about the puppy's details, lineage, or health history. Legitimate breeders will usually provide extensive information and documentation.

Pressure to Buy Quickly: Legitimate sellers won't push you into a decision.

No In-Person Meeting Allowed: Scammers often refuse to allow in-person visits or video calls to see the puppy, giving numerous excuses.

Rudolph the Red Flag Reindeer's Advice

Research Breeders and Sellers Thoroughly: Look for reviews or testimonials and verify their website and contact details. Reputable breeders often have established presences on social media or registered listings with animal organisations.

Ask for a Video Call: Request a live video call to see the puppy. If the seller refuses or makes excuses, it's likely a scam. Reputable breeders should be willing to show you the puppy's environment.

Use Secure Payment Methods: Pay with a credit card or through a secure, traceable method.

Check Photos: Use reverse image search tools (like Google Images) to see if the puppy photos appear on multiple sites, as scammers often steal images from other websites.

Visit in Person if Possible: The best way to ensure you're dealing with a legitimate breeder is to visit in person. If you're unable to travel, consider asking someone in the area to visit on your behalf.

Charity Scams

Christmas is a season of giving, and charities rely on people's generosity to support their work. Sadly, fraudsters take advantage of the 'season of goodwill' and often use fake charity appeals to target those wanting to help others.

How the Scam Works
Charity scams come in various forms, often using realistic logos, websites, and messages to impersonate real charities or false ones. Here are some common ways scammers operate:

Phishing: Scammers send emails or texts pretending to be from well-known charities. These messages link to fake donation pages that steal your personal and payment information.

Fake Websites: Some scammers create fake charity websites or copy real ones, often advertising on social media to reach as many people as possible.

Street and Door-to-Door Collections: Some fraudsters pose as charity collectors in public spaces or go door-to-door asking for donations.

Crowdfunding and Social Media Appeals: Using emotional stories and images, scammers create fake charity pages or crowdfunding campaigns, urging people to donate urgently.

Phone Calls: Scammers may call, posing as charity representatives and requesting donations or sensitive details over the phone.

Warning Signs of a Charity Scam

Unfamiliar or Vaguely Named Charities: Scammers often use names that sound like real charities. Be wary of names that seem unfamiliar or generic.

Pressure to Donate Immediately: Scammers often use high-pressure tactics to prevent you from double-checking their claims.

Unusual Payment Requests: Be cautious if asked to pay in gift cards, cryptocurrency, or bank transfer instead of secure, traditional payment options.

Vague or Incomplete Information: Legitimate charities provide clear, detailed information about their mission, finances, and contact details. If this is lacking, then this a red flag.

Poor Grammar or Spelling Errors: Fake charity emails and websites often contain mistakes or seem hastily put together.

Rudolph the Red Flag Reindeer's Advice

Research Before Donating: Use the Charity Commission website to check if a charity is registered and legitimate.

Donate Directly to Known Charities: Instead of following links in emails or social media posts, go directly to the official website of a charity you know and trust.

Ask for the Registered Charity Number: Legitimate UK charities display their charity registration number, which you can verify on the Charity Commission website.

Be Careful with Cash Donations: If approached in public or at home, ask for identification and details. Reputable charity workers carry ID and will respect your caution.

Verify Crowdfunding Campaigns: Research the person or organization running the crowdfunding campaign, especially if it's new or unfamiliar.

Avoid Giving Out Information Over the Phone: Do not provide sensitive or payment information to callers claiming to represent a charity. Request information by post or direct to the official charity website.

Fraudsters aren't taking a holiday - protect your voice this festive season!

With the Christmas and New Year season fast approaching, life can become increasingly hectic. When we're busy, we're more vulnerable to fraud. As new technology continues to develop, fraud risks are constantly evolving.

You may have seen the BBC news article about how a journalist has been able to replicate her voice using Artificial Intelligence, which was then used to bypass voice ID to gain access to a bank account. If you missed the article, you can read it here - Cloned customer voice beats bank security checks - BBC News

Software is readily available to use to recreate somebody's voice. In this day and age of TikTok, Facebook etc, as well as professional corporate videos, it isn't difficult to find a short clip of somebody speaking which is all that is needed to clone them. A few seconds is enough to create a deepfake that will 'say' whatever it is programmed to.

What does this mean for NHS staff? We have already seen numerous instances when scammers have contacted us pretending to be a supplier, from a bank etc. In these instances, it would be rare for the call receiver to actually know what the person sounds like and so usual advice will apply about making independent checks. The concerns we have are more for if a senior member of staff had their voice cloned and used to request an unexpected urgent payment to be made to a "new supplier".

Rudolph the Red Flag Reindeer's Advice

If you do receive a voice call from somebody you know, and the request is unusual / suspicious, please verify it by other means, such as calling back on a known number or dropping into their office in person. Treat requests for payment via the phone the same as if you would via email.

For personal security, such as banking, we would recommend that you do not rely on voice recognition alone. It can easily be replicated and shouldn't be relied upon to keep your assets and information safe. Only use it alongside other security measures.

Avoid a Christmas Catastrophe - Watch Out for Scam Texts

As the holidays approach, fraudsters are busy trying to dampen our festive cheer with scam texts claiming to be from trusted organisations like the NHS, banks, and shopping websites. In all cases the sender had disguised their number to make themselves look like a genuine organisation.

The texts had links embedded in them which would likely have taken the recipient onto a phishing site where their personal / financial details would be stolen. You can't hover over text links like you might in emails to see their true destination, which makes them especially sneaky.

The good news is that receiving a scam text isn't dangerous. How you handle it is what matters.

Rudolph the Red Flag Reindeer's Advice

- **Don't reply.** Whether it's a "STOP" or any other response, engaging with unsolicited texts can make you a target for future scams.
- **Don't click on any links.** Scam links might lead to fake websites or install malware on your device, stealing your information faster than Santa delivers presents.
- **Forward the scam text to 7726.** This spam reporting service helps to keep others safe.
- **Contact the organisation directly.** If someone claims to be the NHS, your bank, or an online store, reach out using the official contact details from their website or a trusted source.
- **Block the number.** Give scammers the cold shoulder by preventing them from contacting you again.
- **Delete the text.** Out of sight, out of mind — clear it from your inbox so you won't accidentally open it later.

If you've lost money or suspect your device has been compromised, don't fret—help is at hand! Report the incident to Action Fraud or call 0300 123 2040. Let's all do our part to keep Christmas merry and bright by staying vigilant against scammers.

REPORTING FRAUD CONCERNS

Fraud vs the NHS

If you think that fraud may be being carried out against the NHS, please notify your Local Counter Fraud Specialist. You'll find our contact details in your organisation's Anti-Fraud, Bribery and Corruption Policy,. You can also report your concerns to the NHS Counter Fraud Authority using their online reporting tool or phone number: 0800 028 40 60.

If you choose to make an anonymous report, please give as much information as possible as we won't be able to get back in touch with you to clarify anything.

Suspicious Emails

Do not click on any links or attachments.

If you have received a suspicious email to your **@nhs.net** email account, you can forward it (as an attachment) to **spamreports@nhs.net**

If you are not sure how to forward an email as an attachment, contact the LCFS team and we will help you.

If you have been sent a suspicious email to another type of email account (not @nhs.net) you can forward it to **report@phishing.gov.uk**

Suspicious texts

Do not click on any links in the suspicious text message.

You can forward suspect text messages to 7726.

Fraud against a member of the public

These concerns can be reported to **Action Fraud (0300 123 20 40),**

If the person has lost money, it may also be appropriate to report the matter to **the police.**

If you suspect that the person's bank account has been compromised, it is important that they **speak to their bank** as a matter of urgency.

I've read the options but I'm still not sure what to do

The Local Counter Fraud team will be happy to advise.

Our contact details can be found in your organisation's Anti-Fraud, Bribery and Corruption Policy.