NOVEMBER 2024

COUNTER FRAUD NEWSLETTER

International Fraud Awareness Week

International Fraud Awareness Week aims to increase everyone's understanding of what fraud is, how it affects us, and what we can do to prevent it. The goal is to empower people to protect themselves, their friends and family, and their workplaces against scams and fraudulent activity.

This year, the Audit Yorkshire Counter Fraud team is focusing on helping people understand fraud risks they might encounter at home. From online scams to fake investment offers, fraud is a common threat in our everyday lives.

By recognising these risks at home, you can build the skills to spot potential fraud situations in your personal life—and bring that knowledge back to the workplace, making it safer too.

Throughout the week, the Audit Yorkshire team will be sharing information and tips to help everyone become more fraud-aware. Follow us on X (Twitter) for daily posts, @AYCounterFraud.

You can also access more information and advice about fraud prevention by checking our previous newsletters, and by visiting the websites shown to the right.

Useful Resources

Action Fraud

National Cyber Security Centre

Which Scam Alerts

Beware of Black Friday Scams

Previously, bargain hunters have lost around £10 million a year to scams during Black Friday.

With AI generated scams making it easier for criminals, the figure could be even higher this year.

Protect your hard earned cash and follow these top tips to shop safely:

Beware of low stock offers. Stating that something is in demand and there is a limited supply may be a warning flag. Scammers want people to act under pressure as they are less likely to think rationally.

Limited time deals can be designed to make you commit before you think. Be wary.

Always use a credit card if possible when shopping online as you will have more protection if things go wrong.

Current events help scammers pick their moments, and Black Friday is one of the times of year when they will try to exploit you as they know people will be keen to snap up a bargain.

Keep your personal details secure, don't share your banking information and passwords.

Fake social media adverts will crop up during black Friday. Ask yourself if the company is legitimate, if the website matches what you'd expect to see, and whether the offers are too good to be true.

Reliable brands and sellers are safer to use. If you've not shopped with the brand before, check TrustPilot and other review sites first.

Imitation goods and counterfeit or low quality products often make an appearance this time of year. Remain cautious of that Cartier watch being sold for £20.

Don't click on links in unexpected emails with bargain shopping offers.

Act quickly if you think you may have fallen for a scam. Tell your bank straight away.

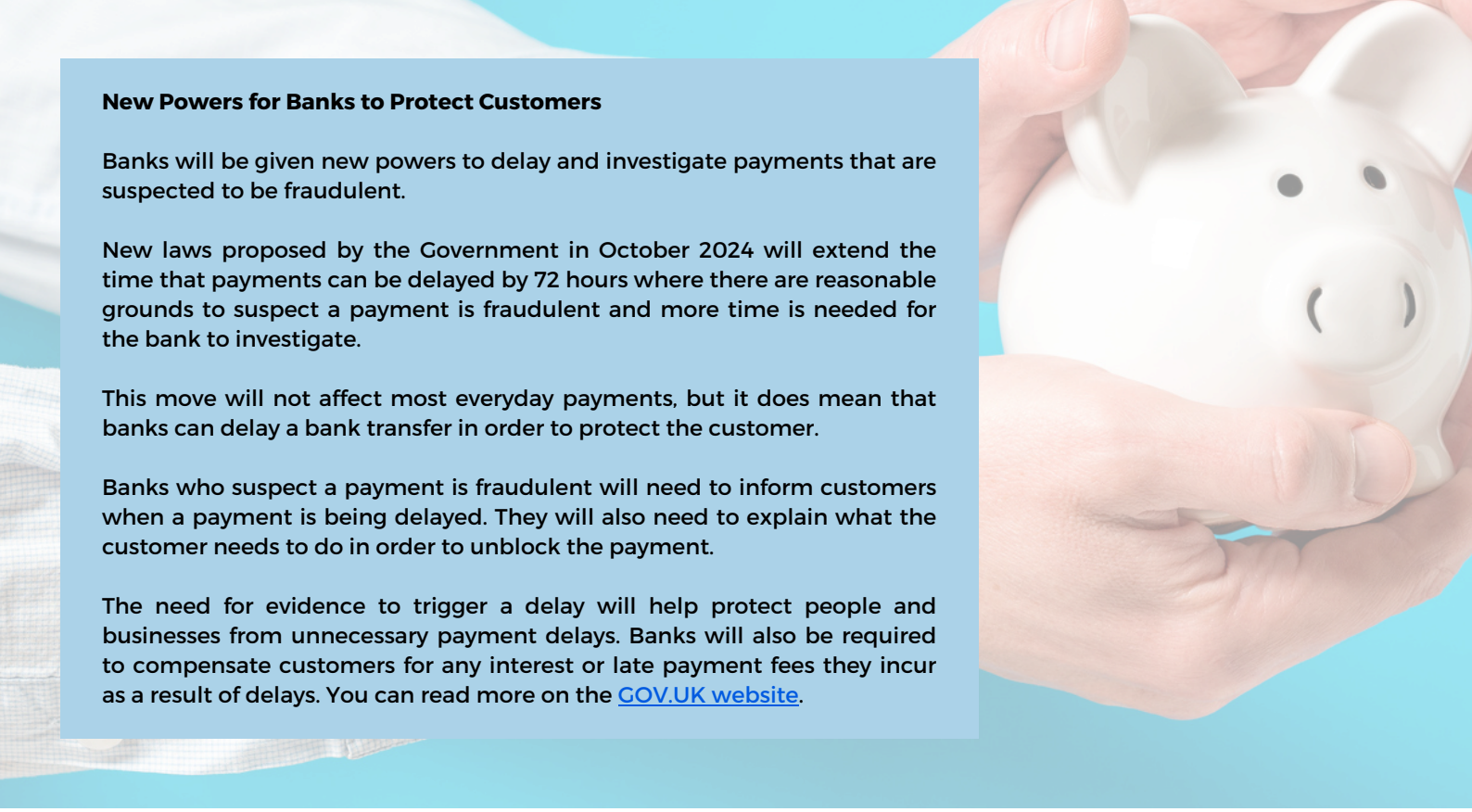
You can relax knowing you've shopped safely if you have followed the advice in this article.

Scam Trend - Fake "NHS Dentist" Posts on Social Media

A new scam trend has been spotted doing the rounds on social media. Fraudsters are posting adverts for new dental practices in local Facebook groups. The posts use artwork / branding / names of genuine dentists, and feature links to websites that look professional.

People who click through onto the fake dentist website are asked to enter their personal details (including passport numbers in some cases) and to make a payment to register or to pay for future treatment. This particular scam has been spotted in Yorkshire recently.

Advice issued on a recent BBC article about the scam includes to always use the official NHS Find a Dentist service when looking for a new practice. Please also be very wary of posts on social media, especially if you find yourself on a website that asks for personal data or payment. Consider registering in person if the dental practice is new and you didn't find them using the official NHS service.



New Powers for Banks to Protect Customers

Banks will be given new powers to delay and investigate payments that are suspected to be fraudulent.

New laws proposed by the Government in October 2024 will extend the time that payments can be delayed by 72 hours where there are reasonable grounds to suspect a payment is fraudulent and more time is needed for the bank to investigate.

This move will not affect most everyday payments, but it does mean that banks can delay a bank transfer in order to protect the customer.

Banks who suspect a payment is fraudulent will need to inform customers when a payment is being delayed. They will also need to explain what the customer needs to do in order to unblock the payment.

The need for evidence to trigger a delay will help protect people and businesses from unnecessary payment delays. Banks will also be required to compensate customers for any interest or late payment fees they incur as a result of delays. You can read more on the GOV.UK website.

New Romance Scam Tactic Spotted

We've all heard the stories of people looking for love online being duped into parting with their money after their potential suitor battles some personal crisis which requires money. There's lots of advice out there to make sure that people don't send money to somebody they have never met. The people committing these scams have also heard this advice and so they have had to up their game.

Earlier this year, we heard of a woman who was a victim of a new romance fraud technique. After chatting online and on the phone, the lady's love interest allegedly went abroad on business. Days later, he contacted his victim with a tale of being beaten up during a car jacking.

In days gone by, at this point, the fraudster would have asked his new love to send money for hospital bills. Instead, he gave her access to his online banking and encouraged her to move money for him. This not only allowed her to see that he was very wealthy, but that he trusted her and was not expecting her to foot his medical bills.

The victim logged onto what looked like a genuine online banking website (it was later found to be fake). At his request, she made some transfers for him. When he asked her to access the account again later, she received a message to say that she had been locked out.

It was at this point that he asked that she foot a bill for him and he would pay her back when his account was unlocked. Believing that this man had plenty of his own money and that it was her fault his bills could not be paid, she agreed. It didn't stop there though, and he duped her into paying more and more bills, totalling £80,000.

He then asked her to put her details into his banking app so he could pay her back, but the transaction never went through. Instead, she was contacted by somebody pretending to be her bank asking her to move more money. It's likely that the information she put into the fake website was used to make this appear to be genuine. It was at this point that the victim realised she had been scammed.

Whilst we don't want to dampen a budding romance, we do ask that if you are dating, online or otherwise, make sure that you get to know the person and be confident you really know their identity before you give out any money.

Romance scams are often underreported as people feel ashamed at having a broken heart and an empty bank account. If you have been a victim, please do seek help, from friends and family, Action Fraud, your bank or the police. You may be able to recover money lost and stop somebody else from going through the same.

Dating fraudsters use fake banks to con woman out of £80K - BBC News

New Tactic - Email QR Phishing

The Counter Fraud Team have been made aware of a phishing email which was received by a senior NHS employee. The email was designed to look as though it had come from a colleague, and asked the recipient to review an important document and pay an invoice.

Where a standard phishing email would usually include a link, this email had a QR code which the employee was encouraged to scan.

We believe that the fraudsters have decided to use this tactic because:

- To open the QR code, the recipient has to use a phone. Phones may not have the same level of protection as our work devices.
- When you receive an unexpected hyperlink in an email, you can check it by hovering over the link with your cursor. This doesn't work with QR codes.
- When you point your camera at a QR code, you'll see the start of the web address - but you might not be able to see the full link. This makes it harder to verify if the link is genuine.
- The presence of a QR code can make an email feel more official. In reality, anyone can make a QR code quickly and easily. They are no more official than a standard hyperlink.

Please be very wary of emails received which ask you to scan a QR code, they could be trying to divert you away from secure systems and support.

If you are unsure about an email you receive at work, please contact your IT team or speak to your Local Counter Fraud Specialist for advice,

Spotting Artificial Intelligence Scams

If you're a regular reader of this newsletter, you will know that the Counter Fraud team are very interested in how Artificial Intelligence (AI) impacts on fraud. As with all new and emerging technologies, AI tools can be used for crime.

For example, fraudsters can use tools like ChatGPT and its competitors to generate high quality written content for phishing emails. Deepfake software can be used to create convincing fake footage of celebrities endorsing bogus investment schemes. A person's voice can be hijacked and used to target their relatives over the phone.

Which? the consumer advice organisation, has put together a fantastic guide on how you can spot and avoid AI scams. A very quick summary of how to spot AI enabled scams can be found below, but we would encourage you to visit their website to read the guide in full.

Deepfakes

Lip syncing is slightly off

Blinking doesn't look right

Body movements don't look natural

Odd background noises

Voice Hijack

Person doesn't say much

Try laughing - AI often doesn't know how to respond

You are asked to send payment in cryptocurrency or gift cards

Phishing

Senders email address isn't right

Email is trying to rush or panic you

No personal greeting

Links to unknown websites

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.