MARCH 2025

AUDIT YORKSHIRE

COUNTER FRAUD NEWSLETTER

Welcome to our Counter Fraud Newsletter. We hope you find the contents helpful. As always, if you need any fraud advice please reach out to your Local Counter Fraud Specialist. You'll find our details in your organisation's Anti Fraud Bribery and Corruption Policy.

Fraud Outlook for 2025

CIFAS recently shared their predictions on the state of fraud in the UK for 2025, and it's a bit of a mixed bag. While 2024 saw a 10% drop in fraud, early signs suggest that things might level out—or even get worse—heading into 2025.

Fraud against businesses, especially in sectors like telecommunications and online retail, continues to grow. And it's hard to talk about fraud these days without mentioning AI. Unfortunately, AI doesn't just promise innovation; it also poses a huge threat by making fraudsters more sophisticated and harder to catch.

This is bound to keep Lord Hanson, the UK's first Fraud Minister, busy. Luckily, there are some important initiatives in the pipeline for 2025 that should help tackle the issue head-on.

Ofcom's Illegal Harms Codes of Practice

Starting mid-March, tech platforms and search services will be required to step up their game in preventing fraud, as part of the Online Safety Act 2023. If they don't, they could face serious consequences.

This is a big deal for social media and search companies, who'll need to make sure they're taking real action to keep fraudsters at bay.

Data Use and Access Bill

The government's Data Protection and Digital Information Bill has had a revamp. If passed, this new law will create a framework that makes it easier to share information when it comes to preventing fraud.

Essentially, it should clear away any red tape that's been getting in the way of sharing data to stop fraudsters in their tracks.

The UK's Fraud Strategy

We're also expecting a new UK Fraud Strategy by the end of the year. This will likely cover all types of fraud—from consumer scams to attacks on businesses and the public sector.

Prevention and data-sharing will likely be at the core of this strategy, helping everyone work together more effectively to fight fraud.

Policing and Fraud Response

Historically, policing has focused on street-level crime, often overlooking the growing threat of online fraud.

But with nearly half of all crime now taking place online, it's clear that the government will need to rethink how it tackles fraud in the digital world.

Fraud isn't just a local problem; it's global. That's why the UK will need to look beyond its borders and work with other countries to fight it. This could involve setting up cross-border partnerships and offering technical assistance to countries where a lot of the fraud originates.

In short, while the growing role of AI and the global nature of fraud are real concerns, there are also plenty of positive developments in the fight against fraud. With the right measures in place, we're on track to tackle these challenges head-on in 2025.

Beware of Scam Calls on Work Phones

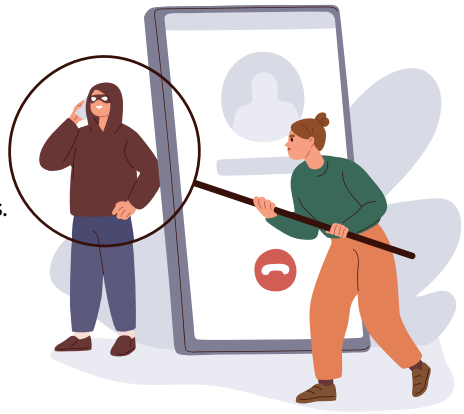
A staff member at a local hospital recently received a scam call on their work landline. It was an automated message claiming their bank card had been used on Amazon for the first time and needed verification.

The employee reported it to their Local Counter Fraud Specialist. This serves as a reminder that scam calls can target both work landlines and mobiles—one of our specialists even received a fake HMRC call on their work phone.

How Do Scam Calls Work?

Fraudsters use a technique called spoofing to disguise their phone number. This means the caller ID may show a fake number or even a trusted name, making the call seem legitimate. Never rely on caller display to verify who's calling.

What Should You Do?
Amazon provides helpful advice on their website about spotting scam calls. If you ever feel uneasy speaking to someone claiming to be from Amazon:



✅ Hang up immediately.
✅ Contact Amazon's customer service through their website or app.

Red Flags to Watch Out For
⚠ The caller asks for your payment details, bank info, passwords, or one-time passcodes.
⚠ They claim an expensive order has been placed on your account.
⚠ They may offer a refund you weren't expecting.
⚠ Some fraudsters will ask you to install an app on your device during the call.

Reporting and Protecting Yourself
📞 Report scam calls to Action Fraud (0300 123 20 40) and Amazon (via their website).
🏦 If you've shared bank details or made a payment, contact your bank and let them know.
🚨Use a different phone to call your bank, or wait at least 15 minutes after hanging up to avoid any fraudster interference.

Stay vigilant and report anything suspicious—it helps protect everyone.

More Phone Safety Advice

Securing your phone apps

We should have all heard of two-factor authentication (2FA) to give an extra layer of security when accessing our accounts online, but how many of us have sought it out where it isn't mandatory?

Which? has published a new document on their website to make us think about making our transactions online safer and reduce the chance of fraudsters guessing our username and password combinations to access websites, hijack our accounts to make purchases, steal our details for future use or to sell our information on to other fraudsters. Please follow the link below to find out more:

7 smartphone apps you need to secure right away – if you value your privacy - Which? News

WhatsApp delivery scam

Fraudsters have been targeting WhatsApp users again, this time sending messages which claim to be about a parcel due to arrive from Evri.

The fraudster says that a delivery to you has failed and sends a link to enable a redelivery to be booked. The link is to a website which looks like the Evri one, but it has been set up to harvest the personal and banking details of the recipient.

Which? has published an article which includes screenshots of the scam page. To see these and to read further tips on spotting phishing websites and scam texts please follow the link below:

Scammers use a verified WhatsApp account to carry out new delivery scam - Which? News

CYBER SAFETY CORNER

Don't get 'ad

An average internet user can be exposed to in excess of a thousand online adverts a month. As well as being intrusive, they can be malicious.

When you load up a website, your browser retrieves resources from different locations to load the page, which includes the adverts. An ad blocker will have built in filters to exclude the adverts. In its place, you will get a placeholder or an empty space.

Ad blockers can be linked to a specific browser (browser-based) and only work when you search for websites on that particular browser. Alternatively, you can use a system wide ad blocker which will scan your whole device, not just the browser you are looking at.

Having an ad blocker can create faster webpage loading and make pages easier to navigate without having to scroll past the ads. As well as having an easier to navigate page due to the lack of clutter, ad blockers can prevent accidental malicious downloads. Privacy is also enhanced as some ads will track the behaviour of the user and may also collect personal information.

However, they may distort some web pages, and prevent you from seeing the ads you may have wanted to look at. It can also limit non advert related content on some websites. Blocking ads may also have an impact on people who rely on revenue from the adverts.

Ad blockers may not be able to stop sponsored ads, which are when a business pays for their ads to be displayed prominently on specific platforms. They can be made to appear as content, without advert related metadata which makes it impossible for a blocker to spot.

Some platforms (eg Youtube, Spotify) offer an ad free service for a fee. This allows them to recuperate money they may lose from the businesses paying for their ads to be displayed, whilst also offering users a better experience.

Blockers may already be included in online security packages.

If you decide to instal an ad blocker, make sure it is reputable – it goes without saying that some ad blockers may themselves be malicious. Whether you have an ad blocker or not, be careful about what you click on. Research companies before giving them your hard earned cash or personal details.

Did You Know? The Earliest Recorded Fraud

Although the Fraud Act only came to existence in 2006, fraud and scams have truly been around for millennia.

One of the earliest recorded cases dates back to 300 BCE and involves a Greek sea merchant named Hegestratos.

At the time, merchants could take out a type of insurance policy known as a "bottomry". This allowed them to borrow money against their ship and cargo, with the loan to be repaid with interest after successfully delivering the goods. If the merchant failed to repay, the lender could seize the ship and its cargo as compensation.

Hegestratos, however, had a different plan. He took out the loan but intentionally sank his empty ship, hoping to keep the borrowed money without fulfilling the agreement. His scheme didn't go as planned.

He was caught in the act of sabotaging his vessel, chased by those who discovered his plot, and ultimately drowned while trying to escape.

This ancient case shows that even thousands of years ago, fraudsters were scheming—and sometimes paying the price for it. Hegestratos' failed plan also set the stage for countless insurance scams in the centuries to follow.

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.