JUNE 2024

AUDIT YORKSHIRE

COUNTER FRAUD NEWSLETTER

Welcome to a special edition of our Counter Fraud newsletter for NHS staff. If you need any advice on fighting NHS fraud, please contact your Local Counter Fraud Specialist. You'll find our details in your organisation's Anti-Fraud, Bribery and Corruption Policy.

AI Special

- What is AI?
- How does AI affect NHS Fraud?
- The Rise of AI in Fraud Tools
- Using Generative AI Safely
- Seeing is Believing? Spotting AI generated photos / videos.
- Deepfakes vs Shallowfakes
- How to report fraud

What is AI?

Artificial Intelligence (AI) is a branch of computer science focused on creating systems capable of performing tasks that typically require human intelligence.

These tasks include learning, reasoning, problem-solving, perception, language understanding and decision-making. AI systems achieve these capabilities through various techniques, including:

- **Machine Learning (ML):** A subset of AI where systems learn from data and improve their performance over time without being explicitly programmed.
- **Natural Language Processing (NLP)**: Enables machines to understand, interpret, and generate human language.
- **Computer Vision:** Enables machines to interpret and make decisions based on visual inputs, such as recognising objects in an image or video.
- **Robotics:** Integrates AI with physical robots, allowing them to perform tasks in the real world, from manufacturing to surgery.
- **Expert Systems:** Uses knowledge and inference rules to mimic the decision-making abilities of a human expert in specific domains.

Overall, AI aims to enhance or replicate human capabilities in various fields, leading to improved efficiency, innovation, and problem-solving abilities.

The above article was written using AI. One of the team used ChatGPT and asked it to "write an article explaining what AI is".

When ChatGPT was asked to "explain AI in simple terms", it came up with the explanation in the box to the right.

So there we go – an explanation of AI using AI!

AI, or artificial intelligence, is when computers and machines are designed to think and learn like humans. This means they can solve problems, make decisions, understand language, and even recognise images.

Imagine teaching a computer to do tasks that usually require human intelligence, like chatting with you or playing a game. That's what AI is all about.

How AI can affect NHS Fraud

Hopefully you will now have a better understanding of what AI is. Next, we will look at different areas that it may affect fraud in the NHS.

It is important to remember that using AI is not a crime. It can be used by criminals to help commit fraud more effectively.

Application forms

The Counter Fraud Team has been sent numerous dodgy-looking application forms to review. It is suspected that many of the responses on these have been created with the help of AI. Typing "how can I describe how I am a good team player" or similar into a Generative AI app powered app will come up with a beautifully written response. At the time of writing, there is no 'ban' on using AI to assist in drafting application forms – it is no different to finding samples from Google or asking a friend for advice. In all of these situations, the crux of the matter is to make sure that what is written is truthful.

AI (like Google and friends) can make things up which do not apply to the applicant, and therefore the application form may be fraudulent if it makes false representations. For example, we have seen somebody giving examples of tasks they had done in their role as a Project Manager – but in their work history, they had never had a job as a Project Manager. By contrast, if a Care Assistant asks AI to "list tasks a Care Assistant does" and the applicant chooses only the responsibilities which actually apply to their role to add onto their application form, it would not be fraud.

Phishing emails

Phishing emails are sent to try and trick the receiver into doing something, such as entering their log in details into a fake website or make a payment which is not required.

These emails are often sent from organised crime groups who can be anywhere in the world and poor spelling, terminology and grammar could be indicative that they were not genuine. AI will allow the fraudsters to create personalised and professional sounding emails more effectively.

Invoice fraud

For years, fraudsters have used many techniques to try convincing organisations to make payments for goods and services which have not been received.

AI is going to assist the fraudster in many ways, from analysing publicly available information to spot patterns of spend, to drafting realistic looking fake invoices.

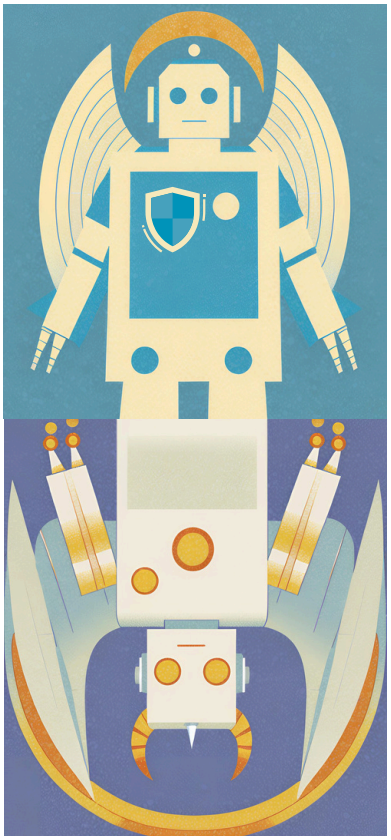
CEO Fraud

Fraudsters impersonating senior staff may become more difficult to spot if AI is used. At present, this will be as described above, with more convincing emails. As AI technology develops, we anticipate that voice recognition and deepfake videos could be used too.

These are just a few ways which AI could be used to assist fraudsters target the NHS. It is important to be aware of this developing risk, but current advice remains the same.

If you are concerned that you may have spotted fraudulent activity or you're unsure about something you have received and need some advice, please contact your Local Counter Fraud Specialist. You'll find our details on the last page of this newsletter.

The Rise of AI in Fraud : New Tactics and Tools for Both Sides



AI tools such as ChatGPT, Google Gemini, Claude and Microsoft Copilot are also known as generative AI. This is because they generate new content. Generative AI can create photos, artwork, voice content, music and documents. In fact, all of the artwork in this edition of the newsletter is AI-produced.

There is now a product sold on the dark web called FraudGPT, which allows criminals to make content to facilitate a range of frauds, including creating phishing emails, or to custom-make scam web pages designed to steal personal information.

The use of voice cloning is also a growing issue- it can be used to convince a relative that a loved one is in need of financial help, or even in some cases to convince them the individual has been kidnapped and needs a ransom paid.

Reports of AI tools being used to try to fool banks' systems have increased significantly, according to anti-fraud organisation CIFAS.

AI as a Fraud Fighting Tool

It must be remembered that AI is also used to combat fraud. Many industries use AI for fraud prevention and detection purposes. This can be done by:

- Analysing vast amounts of data to spot patterns and anomalies.
- Monitoring behaviours and flagging anything which deviates from this.
- Verifying identity, such as facial recognition.
- Analysing text and speech which can help identify phishing emails.
- Anything suspicious which is spotted can be actioned by AI.
- Predicting fraud risks in future by looking at historical data and trends.

As we highlighted in our May edition of this newsletter, the UK government uses AI-enabled analysis of public sector data to prevent and detect fraud.

AI Checkers

If you want to check if something is likely to have been AI-generated, there are plenty of online AI checkers available. Simply search "check if text / picture / video is AI generated" and you'll find lots of free tools. Be mindful that these services are still developing and they may sometimes get it wrong. It is likely that their accuracy will increase over time - the Counter Fraud Team has noticed an improvement in these services in the past 12 months.

Using Generative AI Safely

Having generative AI tools such as ChatGPT within easy reach can be extremely helpful. AI has exciting potential in terms of solving problems, increasing efficiency, and improving lives. However, there are also pitfalls if used without considering the risks.

Privacy – anything that is shared with openly available AI platforms can be stored and become part of the systems knowledge base. This includes the requests you make and any data you share. Sharing other people's information with AI could constitute a data breach. Uploading business sensitive data could represent a breach of confidentiality.

Hallucinations – generative AI can hallucinate. A lawyer in New York fell foul of this when he asked AI to help him find case citations for a court case. AI created imaginary cases which the lawyer then presented in court as case law. As you can imagine, the courts took a very dim view of this incident and the law firm were fined $5,000.

Inaccuracy and Bias – AI tools such as ChatGPT are trained on data from multiple sources. These sources may be biased or inaccurate, resulting in AI parroting ill-founded information. There are concerns that AI tools may exclude less obvious information, and that it tends to be poor at weighing up strengths and weaknesses of source data.

Trust – the ability to detect AI-generated content is a hot topic at the moment, as AI generated false information are highly dangerous tools for criminals who look to manipulate people. Improving online safety and preventing the spread of false information is a top priority for governments and law makers. As detection tools get better AI-produced content may be detected. If you have not been transparent about how you have used AI, this may undermine trust.

It is important to be aware of the limitations of AI tools. If you are considering using AI at work, **you must ensure that you follow your organisation's AI Policy.** If they do not have an AI policy, please seek guidance from your organisation's Information Governance and IT teams before using AI.

Seeing is believing?

Spotting AI Generated Images and Videos

Experts have begun referring to nonsensical AI generated content which is clogging up social media as "slop". It appears that bots are churning out large quantities of AI content simply to attract clicks and internet traffic.

There are also real concerns that criminals may use AI to produce fake content (disinformation) in an attempt to disrupt other countries - particularly during elections. Disinformation is deliberately incorrect and is aimed at misleading the viewer.

As both the UK and the US move towards major elections, there is a higher potential that you will encounter disinformation and misinformation (which is false information which is shared by someone who doesn't realise the information is not genuine) on social media.

So, how can you spot an AI generated fake video or photograph?

Photographs

- **Unnatural details**. AI generated images often have subtle imperfections that give them away. This includes things like unnatural lighting, strange anomalies in the background, and people / objects in the image may have fuzzy or unusual edges.
- **Eyes and hands.** AI struggles with complex details such as hands and eyes. You might notice that a person's eye colour is not as expected or that their hands are distorted.
- **Shadows.** The image may look slightly off as a result of shadows not matching where the light is supposed to be coming from.
- **Context and source.** Consider where the image has come from. Reputable media outlets are much less likely to use AI generated images without being transparent about it. Social media companies cannot control all the images that are posted on their platforms, and users with an ulterior motive are unlikely to announce that they are posting a fake image.

This photo was generated using the prompt "Woman enjoying a sunny day in London".

From a distance it looks OK, but let's look closer...

The edges of the hands holding the frame are poorly defined and the fingers are extremely long.

If you zoom in on the figure in the central photo, you can spot many distortions in her appearance and clothing.

Once you zoom in you'll also notice significant issues with the background of the photo. There are random parts of cars, Big Ben looks like it could be made out of Weetabix and the windows of the building behind the person are distorted.

Videos

- **Lip syncing issues** - the audio of the video may not line up properly with the person's mouth movements.
- **Unnatural blinking patterns** - the person may be blinking in a predictable frequency or not blinking at all.
- **Facial expressions may be jerky** - going from straight faced to smiling and back again at random times with no natural graduation between expressions / lacking a shift in tone of voice at the same time.
- **Eyes** - the person's eyes may show unusual reflections or lighting, or may not move in the way we'd normally expect.
- **Background distortion** - as with the photo we just looked at, you might need to zoom in to spot these discrepancies. The background might be distorted, especially around the main subject of the video.
- **Light and shade** - the lighting in the video may seem unnatural and shadows may not align with the apparent source of light.
- **Context** - again, consider the source of the video and if the behaviour seems out of character for the individual consider whether it could be a deepfake.

In the News

Martin Lewis Deepfake investment scam warning

Company loses $25 million via Deepfake conference call

You've heard of deepfakes, but what about shallowfakes? Read on to find out what these are in the next section.

Deepfakes vs Shallowfakes

You may have seen in the news that fraudsters are editing images of vehicles to show that they have been damaged in order to claim insurance payouts. These are often termed as being created using 'shallowfake' technology. We have been bombarded with news articles about deepfakes – so what's the difference?

A **'deepfake'** is a photograph, video clip or audio recording which has been created with sophisticated AI software.

A '**shallowfake**' is media which has been altered but without the use of AI. An example may be the use of a photo editing suite such as Photoshop.

While the name shallowfake may make it seem to be less harmful than deepfake, it can be equally as damaging. Fraudsters can create shallowfake ID documents, invoices or bank statements.

Read this article to discover how a small business owner had claims made against him when images of his van from social media were shallowfaked to make it look as though it had been involved in an accident.

Be mindful of what you post on social media – we've seen what can happen to images of vehicles in the article above – but think what else could be doctored and used for no good.

Never post images of ID badges, concert tickets or receipts for purchases you're excited about. Also make sure that your social media is secure, allowing only people you know and trust to view it.

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.