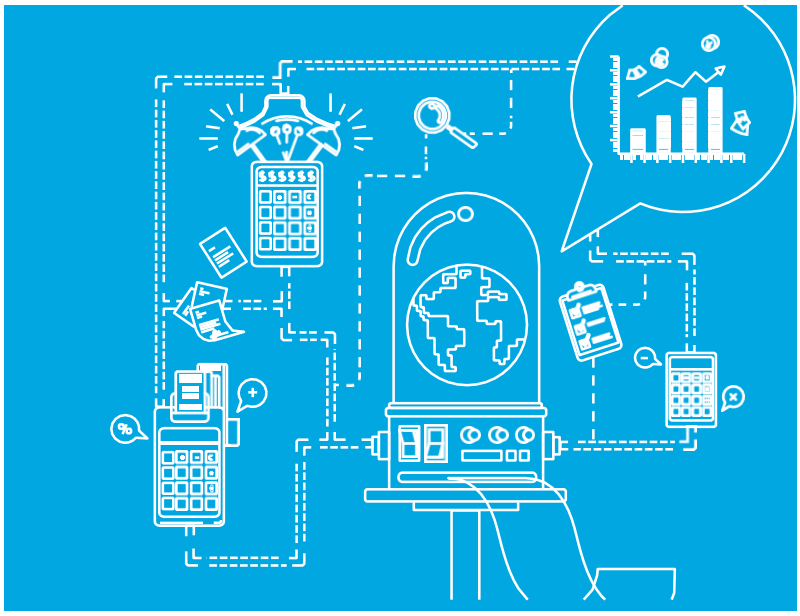
Notice Fraud
April 2020



COVID-19 Fraud

Fraudsters are exploiting the spread of the COVID-19 coronavirus to facilitate various types of fraud and cyber-crime. Figures show, as of 20th March 2020, there have been 105 reports to Action Fraud with total losses reaching nearly £970,000. Reporting numbers are expected to rise as the virus continues to spread across the world. (Source: Action Fraud)

Some common scams we have seen include:

- purporting to be from HMRC offering a tax refund and directing victims to a fake website to harvest their personal and financial details.
- SMS messages detailing government fines for leaving the house.
- links to documents detailing fake cures, that require a link to be clicked on.
- purporting to be the WHO or US CDC to provide medical advice, or request donations to aid research in the form of bitcoin payments
- providing articles about the virus outbreak with a link to a fake company website where victims are encouraged to click to subscribe to a daily newsletter for further updates.
- sending investment scheme and trading advice encouraging people to take advantage of the coronavirus downturn.
- sending requests for prompt settlement of fake invoices.

There have also been over 200 reports of coronavirus-themed phishing emails in just a few weeks (Source: Action Fraud). These attempt to trick people into opening malicious attachments which could lead to fraudsters stealing people's personal information, email logins, passwords, and banking details.

Do not open any email that looks suspicious and be aware that scams and phishing attempts can also come from text messages, phone call or social media contacts.

Here are some ways to help protect yourself and your organisations against fraud at this difficult time:

Watch out for scam messages:

Don't click on the links or attachments in suspicious emails, and never respond to unsolicited messages or calls that ask for your personal or financial details.

Shopping online:

If you're making a purchase from a company or person you don't know and trust, carry out some research first, and ask a friend or family member for advice before completing the purchase if you are unsure. If you decide to go ahead with the purchase, use a credit card if you have one, as most major credit card providers insure online purchases. For more information on how to shop online safely, please visit: https://www.actionfraud.police.uk/shoponlinesafely.

Protect your devices from the latest threats:

Always install the latest software and app updates to protect your personal devices from the latest threats. For information on how to update your personal devices, please visit: https://www.ncsc.gov.uk/guidance/securing-your-devices.

Threats against staff to obtain ID badges

We have received notification from several NHS organisations that staff have been threatened at knife point for their NHS badges/IDs.

Please ensure that you do not display your ID badge when outside and only leave buildings via public entrances, accompanied (observing social distancing rules) unless you have no alternative.

Continue to be alert and report any suspicious activity, as always, to your organisations' Local Counter Fraud Specialist.

New Risks and Other Scams

Voice spoofing

There is currently a new tactic being used by fraudsters where they can spoof/imitate voices of key staff in order to contact junior staff within an organisation via telephone and instruct payments to be made, or suppliers set up.

The fraudsters will initially make contact with the victim and ask them seemingly innocuous questions, which are being recorded. Once they have sufficient voice material recorded, they can use free opensource software to replicate the voice using any script they write. This is then used to telephone others and commit fraud, by requesting personal details, requesting payments be made, or suppliers set up. The spoof is so good that the person receiving the call would not be able to distinguish between the voices.

You should be wary of unusual requests made over the phone and seek additional authority through conventional methods, not email, but to use internal skype or a new phone call to the recognised number of the apparent approver.

Job Offer Scam

Fraudsters are currently targeting people with fake job offers from NHS Trust's.

They contact victims, claiming to be from the Recruitment Department having received the applicants resume and request personal details including full name, place and date of birth, and passport details, as well as education certificates. They may also request the applicant pay for accommodation deposits, or insurance premiums.

Trusts should help protect themselves from this by putting a warning on official websites to highlight that they do not request money from applicants, and jobs are advertised only through NHS jobs.

Benefit Payment Email

Emails are currently circulating around some organisations asking for staff to verify their email account to "avoid omission of your benefit payment for March 2020". This includes a link for staff to click on to enter their personal details, for fraudsters to collect this information. Please do not click on these links and report any of these emails immediately to your Action Fraud at https://www.actionfraud.police.uk/.

Recent Cases

A London GP was found to be self-prescribing Tramadol using a patients' record. They were adding the prescription to the patients' record, submitting online and collecting from a local pharmacy on the pretence it was for the patient. They admitted the drug was for their own use during their interview under caution.

The GP pleaded guilty and was sentenced to a community order of 100 hours unpaid work, to be undertaken within 12 months, and a 10-day rehabilitation order. She was also ordered to pay £47.51 compensation, £85 court costs and a victim surcharge of £85 with ongoing action by the GMC.

Reporting concerns

Don't be embarrassed to report a scam. Fraudsters are cunning and clever; there is no shame in being deceived. By reporting, you will make it more difficult for them to deceive others.

It is easy to report fraud or bribery affecting the NHS:

Contact your Local Counter Fraud Specialist (LCFS)
or
call 0800 028 4060
or
visit https://cfa.nhs.uk/reportfraud

It is the LCFS' role to take every allegation of fraud or bribery seriously and to provide anonymity and confidentiality for anyone who reports a concern. It is recommended that you refer to your organisation's policy on fraud when reporting allegations for further information on how you are protected. When making a referral please provide as much information as possible, for example:

the name of the person who you believe has committed a fraud:

- when and where the fraud has taken place;
- how long the fraud has been going on; and
- any details to substantiate your suspicion.

Remain vigilant during this uncertain period.

Spot it. Report it. Together we stop it.