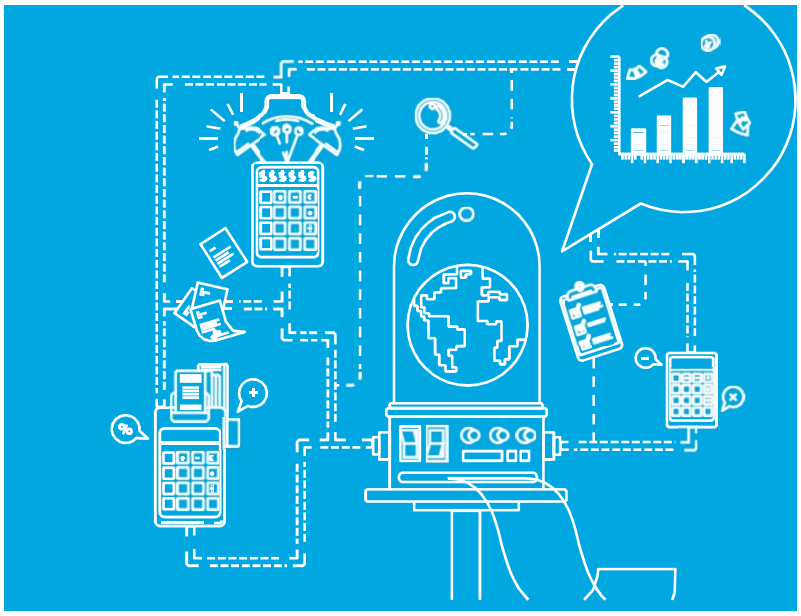
Notice Fraud February 2020



Phishing scams

We have all heard or seen the emails from a company you trust for example banks and credit card companies asking you to update your details or risk your account being suspended. Examples include rebates or penalties from HRMC, TV Licencing, PayPal, or Netflix. This is known as phishing – it's a method used by fraudsters to trick you in to handing over personal or sensitive information using legitimate looking emails and websites.

More recently we have seen an increase in phishing emails being sent to work email addresses. One of latest scams looks like it has come from payroll or the payroll self-service site with details about a pay rise. A link in the email takes users to a copycat website which is controlled by the fraudster. Once login details are entered, the fraudsters use these to change bank details for future salary payments.

How can you identify a potential phishing email?

Phishing emails can often (but not always) contain some of the following characteristics:

- The sender's email address doesn't tally with the trusted organisation's website address.
- The email contains spelling and grammatical errors.
- The email does not specifically use your name but uses a non-specific greeting like 'dear customer'.
- A sense of urgency, for example the threat that unless you act immediately your account may be closed.
- A prominent website link. These can be forged or seem very similar to the legitimate address, but even a single character difference means a different website.
- A request for your personal information such as username, password, employee number or bank details.

What should you do if you suspect you have received a phishing email?

Please do not open suspicious emails, attachments or click on or open anything, even if it purports to come from a colleague or known correspondent. This may trigger something dangerous to your PC or the organisation's network. If you receive a suspicious email:

contact your local IT service desk of the attempt, so that the email address can be monitored when used;

- do not reply to the email or contact the senders in any way;
- do not click on any links or open any attachments; and
- if you have clicked on a link in the email, do not supply any information on the website that may open.

If you have any questions in relation to the contents of suspicious emails, please refer them to your Local Counter Fraud Specialist. Refer to your organisation's anti-fraud policy, email and internet policies for further guidance.

New risks

Fraud prevention notice (FPN) Misrepresentation of qualifications, skills and experience

The NHS CFA have published an FPN in relation to misrepresentation of qualifications, skills and experience following a case identified at a Clinical Commissioning Group, which suffered a loss of £13,171.97. Fraud of this nature exposes the organisation to the risk of employing staff who do not hold the correct qualifications. This could bring reputational harm to the organisation and affect patient safety. The information was circulated to the key organisation contacts with the associated prevention advice.

Scam calls from EDF to NHS organisations

An NHS Trust has received a telephone call from an individual purporting to be calling from EDF Energy. Claiming that their system had suffered a failure, the caller requested the billing information on the Trust's last invoice so records could be updated. The Trust refused to provide the information at which point the caller became argumentative before ending the call. EDF Energy have confirmed that they have no knowledge of any issue which would have prompted a genuine call of this nature.

If any similar calls are received you should obtain as much information as possible but not divulge any, and then report the matter to your LCFS

Two-Factor Authorisation - 2FA

Two-Factor authorisation is the process of requiring secondary authorisation to make a key change such as password or bank details.

Banks and other organisations will send a code to an email address or telephone to ensure the genuine user is aware of the change, but fraudsters have identified ways in which to beat this process. Fraudsters have been discovered contacting fraud victims purporting to be from the bank/organisation. They state that to verify the call and pass through the security process they will send a 2FA code to the victim. At the same time, they go through the password reset / bank change process, which automatically sends the code through. They then ask the victim to read the code back to verify their identity, which they can input to the system and bypass the control.

Please be reminded never to give out your password or a 2FA code over email or the telephone.

Secondary employment / working whilst sick

We continue to see a large number of referrals of staff working whilst sick. Historically this related to staff working at other Trusts or care providers, but the rise in social media has allowed many people to set up home businesses offering massage, personal training, beauty therapy, dermatology, botox, fillers and other medical services. In addition to the risk that staff may continue these businesses whilst off sick from the organisation, the practice of offering medical services from home gives risks of malpractice/negligence. Potentially exposing the organisation to risk by association to the employee where medical related services are provided. It is important that organisations fully understand any additional employment undertaken by their staff, and that the disclosed employment is risk assessed to ensure the organisation has reduced any risk to themselves. All secondary employment should be declared, and risk assessed by line managers.

Recent cases

Working whilst off sick

A nurse from Wales has been jailed for moonlighting whilst on sick leave from her job.

The mental health nurse obtained sicknotes falsely claiming that she was too ill to work with Aneurin Bevan University Health Board in Wales. She told her line manager that she was 'too stressed' to drive to carry out her NHS work, whilst registering with and working night shifts for a privately-run care agency. She worked 53 shifts for the agency between March and November 2018, receiving £18,800 in sick pay in addition to the pay received for the shifts that she worked.

She claimed that she had been told by the Royal College of Nursing that she was allowed to do agency work whilst on sick leave from the NHS, however a recorded telephone call in February 2018 clearly shows that she was given strong advice that she could be committing fraud if she did.

She was sentenced to eight months in jail after pleading guilty to fraud.

source: South Wales Argus, Daily Mail

Fraud by false representation

A Health Care Assistant (HCA) on a ward at a mental health hospital was found to have taken £2,473.78 from vulnerable patients.

Four patients had money taken from their accounts in various amounts from £150 to £1500 after the HCA had taken the patients' bank cards from the safe at the nurses station. The money was spent on theatre tickets, clothes, hotels and international flights.

The HCA was found guilty of three counts of fraud by false representation, and her partner was found guilty of four counts of fraud by false representation. The subject received a six month suspended sentence 100 hours community service and has to pay £500 court costs. The co-defendant, who did not work at the Trust, also received a six month suspended sentence, 100 hours community service and must pay £1000 court costs and £150 victim compensation.

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, bribery or corruption affecting the NHS. Contact your Local Counter Fraud Specialist (LCFS) directly or call the national anonymous, 24-hour reporting line on 0800 028 4060 (powered by Crimestoppers). You can also report online, completely confidentially via 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 the 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.
Spot it. Report it. Together we stop it.