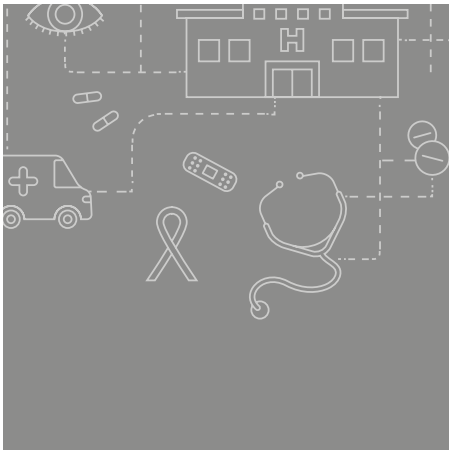

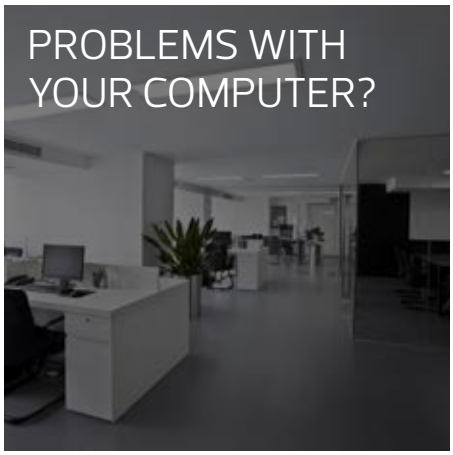

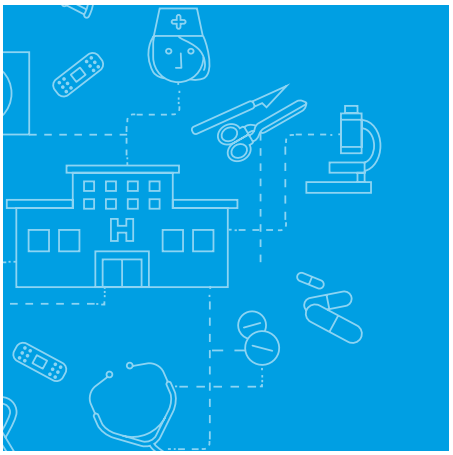

NOTICE FRAUD

This edition of Notice Fraud is designed to bring recent cases or emerging scams to your attention to help you recognise the signs of fraud in the NHS.

NHS WORKER JAILED FOR £93K FALSE IDENTITY FRAUD

A woman who provided false identity documents to secure work as an NHS Student Nurse has been jailed for 16 months, after a joint investigation by NHS Protect and Home Office Immigration Service.

The subject secured NHS employment for eight years using forged and stolen identity documents, false employment references and fake European Union (EU) documentation. The subject was also in receipt of an NHS student bursary to fund their nursing training.

The subject was found guilty of four offences under the Fraud Act 2006 and Identity Documents Act 2010.

UK DOCTORS TARGETED IN BEGGING LETTER SCAM

A handwritten letter is sent requesting money to support a student nurse in Uganda who is struggling to pay her medical school fees. The author states she is a student nurse aged 19, with two younger sisters, orphaned when her father was killed and her mother died from breast cancer. The letter is accompanied by a notice of dismissal letter from St James Medical School, Uganda.

The story is totally fictitious. As the address supplied is a PO box number, the fraudsters pick up the cheques sent by the victim conned into this scam.

The letters are sent directly to the targets workplace which suggests that the fraudsters are targeting specific groups with compassionate instincts. This scam is a variation which initially targeted artists and Church of England vicars.

SUSPICIOUS PHONE CALLS

Be aware of suspicious phone calls in which a man states he is calling from Scotland Yard Fraud Prevention Department. The caller tells the person receiving the call that someone has attempted to use their bank card to purchase an item (in this case a computer) for more than £1,000.

If you receive a similar call to this, please do not give out any personal details including your name, address, card details and PIN number. Hang up immediately.

UNDERSTANDING THE THREAT...

It is unfortunately a fact of life that none of us, organisation or individual, can say that we are exempt or immune from some form of attempted cyber threat.

Naturally, in order to effectively protect ourselves against any form of threat we must first understand the nature of that threat, and the many forms it may take. Below we focus on a form of attack that is worryingly on the increase – Ransomware:

What is Ransomware?
Like most computer viruses, ransomware often arrives in the form of a phishing email, spam, or some other form of nefarious email. You then click a link or open an attachment – the virus then sets to work encrypting your files.

Once the computer is effectively locked down, it demands a fee for the files to be returned.

There is usually a time limit to pay up, after which the ransom increases.

What can you do?
It is actually very simple: be vigilant and use your common sense.

Do not open unsolicited emails, or where you don't recognise the senders email address – if it happened to be genuine the sender will follow up with a call or a second email that's likely to be more easily identifiable.

Do not click on internet links within emails unless you are 100 per cent sure you know where it is taking you, that it's from a trustworthy source and that you are expecting there to be a website link in the first place.

Remember to hover over hyperlinks in emails to verify that the address being displayed whilst hovering matches up to the apparent address of the link itself.

PROBLEMS WITH YOUR COMPUTER?

Fraudsters claiming to be from well-known companies are cold-calling members of the public and stating that there is a problem with their computer or device. The callers then direct the individual to a phishing website that allows them to take control of their computer and download viruses. These fraudsters are the only people capable of removing the viruses and will charge a premium rate to do so.

Do not disclose personal information with organisations or persons, before verifying their credentials. Ensure that your computer or device has up-to-date anti-virus software and a firewall installed.

REPORTING CONCERNS

If you have suspicions that fraud may be occurring or wish to receive further information about the above please contact your Local Counter Fraud Specialist (LCFS).

Alternatively you can report any concerns to NHS Protect on 0800 028 40 60 (between 8am and 5pm, Monday to Friday) or via the online reporting form: **http://www.reportnhsfraud.nhs.uk/** All information provided via this secure website is completely confidential.

It is the LCFS's 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 the organisations policy on fraud when reporting allegations for further information on how you are protected.

rsmuk.com