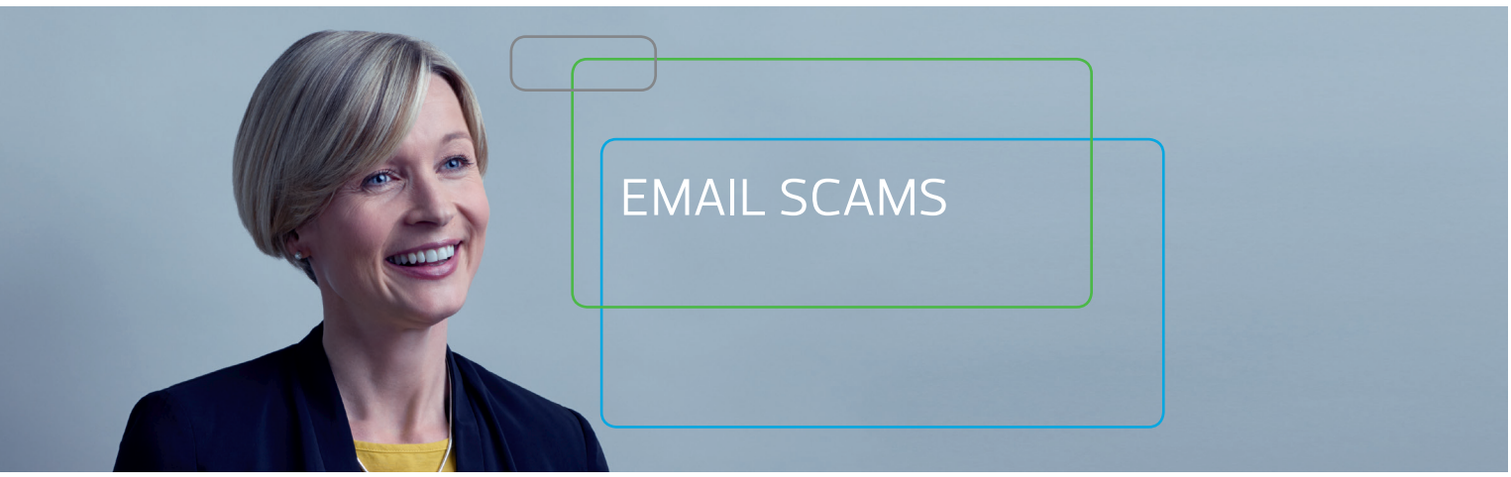

EMAIL SCAMS

Across the healthcare service, we continue to see, on a daily basis, a number of differing cyber related techniques to commit fraud, including email scams.

Email scams appear to resemble genuine and legitimate emails that you would expect to receive. Fraudsters manipulate the email content in order to trick the recipient. As they look just like normal emails, there is nothing contained in them that may trigger spam filters so they arrive at your inbox. They may appear to be from a trusted source, for example:

- another NHS organisation with links to invoices; and
- mobile telephone providers about current bills.

We have seen a number of attempts whereby staff have received emails for bogus invoices or requests for a transfer of funds from the organisation to the fraudster. These particular examples have come in cases where an email scam is sent purporting to be from the organisation's CEO asking for a payment to be made. Fraudsters are using simple methods that resemble day to day transactions. If an email scam is successful, the fraudsters may receive sums of money or obtain access to sensitive and confidential information that could impact the organisation's reputation and finances.

How can you identify a potential email scam?

Fake emails often, but not always, display 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 is sent from a completely different address or a free webmail address.
- The email does not 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 personal information such as username, password or bank details.
- You weren't expecting to get an email from the company that appears to have sent it.
- The entire text of the email is contained within an image rather than the usual text format. The image contains an embedded hyperlink to a bogus site.

The same applies to suspicious or unsolicited letters requesting information or for you to sign up to something on behalf of the organisation without realising. Fraudsters can be sophisticated in their methods and use false telephone numbers, email addresses and even set up false websites, so when you are doing your background research, they appear legitimate. Do not respond to these unsolicited requests. You could provide information that might be used inappropriately or perhaps buy into an agreement without the intention or authority.

What should you do if you have received a questionable email?

Remain vigilant. When you see questionable emails mark them as 'junk' then delete without opening. This way, if you receive communication from the same email address or company again, it will go straight to your junk mail folder where you can safely delete it.

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.