Phishing emails—Don't get hooked!

Most of us receive dozens of new emails a week, at work and on personal email addresses, some of them asking for personal information and in return offering you something that appears too good to be true. If this is the case, then it probably is too good to be true!

Phishing is the name given to the practice of sending emails at random purporting to come from a genuine source operating on the internet to trick you into disclosing information.

Many will ask you to verify or confirm your account or personal information and this will be used by criminals to steal your identity and/or money fraudulently. Another outcome maybe that the emails contain a virus that will harm your computer and the organisations systems or are a hoax used to con and exploit you.

How you can prevent yourself from being a phishing victim:

- Emails may look like they have come from a genuine company or trusted colleague but the name that appears in the 'from' field does not necessarily come from that source and is easy to fake—check the exact wording and spelling as the finer detail may be inaccurate and give you a clue that the email is bogus.
- Emails that appear to come from a senior member of staff instructing for unusual urgent action to be taken, especially in the form of payment, should never be acted upon before confirming with that person by talking to them or contacting them through other means than replying directly to the email.
- If the email was sent out in bulk and addressed generically such as "Dear valued customer..." it is likely they do not know your real name or anything about you.
- Your will never be asked to reveal passwords via email. **Never click directly on to the link on emails from any company always open the web browser** and type in the address yourself as the email link is likely to take you to a false site.
- Don't take any chances! **Always ignore and immediately delete any suspicious emails without opening it or clicking the link provided.**
- Please find a link to a gallery showing phishing emails and how to identify them: http://www.nhscybersecurity.co.uk/awareness/gallery/default.html

If you have any concerns of queries, please contact the organisation's Local Counter Fraud Officer Eleni Gill on **eleni.gill@nhs.net** or call 07827 308906