We have been alerted to bogus ‘phishing’ emails that may be received by registered patients. These emails claim to be from local GP practices and state that access to online GP services has been changed and that patients should log on to their account and update their information.

We would like to remind all local patients to be vigilant and to report any such ‘phishing’ emails and not to click on any links or open any attachments unless they are absolutely certain that the message is genuine. If you do click on any unverified links or attachments you may allow criminals to access your information and/or to corrupt your computer.

Your GP surgery will never send you a message asking you to click on a link to update your details. If in doubt, visit your registered surgery or contact them using trusted contact information.

If you receive an email you should check it for signs that it may not be from the true source it appears to be from.

Check the email address. Is it the same as the email address you usually receive emails from, or just similar?

Check the email subject line. Be suspicious of “There is a secure message waiting for you”, “Security Alert”, “System Upgrade” or similar.

Check the message is personalised with information like your name, your postcode or part of your account number. If it isn’t personalised at all then you should be suspicious. Sometimes the message will contain someone else’s name.

Beware of a prompt to click on a hyperlink or a button, or to download a file – something like “Verify your account or password” or “update your security details”. These will likely take you to a copycat website where you will be prompted to enter your full details.

Be suspicious of any message that creates a sense of urgency, such as “If you don’t respond within 48 hours, your account will be closed”. A legitimate company would never create a false sense of urgency.

Remember, never respond to any suspicious emails and don’t click on any links or attachments within them.

Phishing emails should be reported to: https://www.actionfraud.police.uk/report_fraud