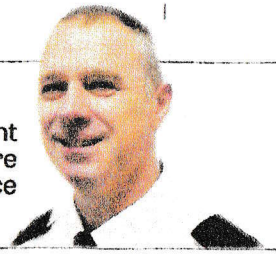
John Wilkinson

Acting Superintendent
North Yorkshire
Police



Be vigilant on increasing threat of fraud

Happy New Year to everyone in all corners of our North Yorkshire communities.

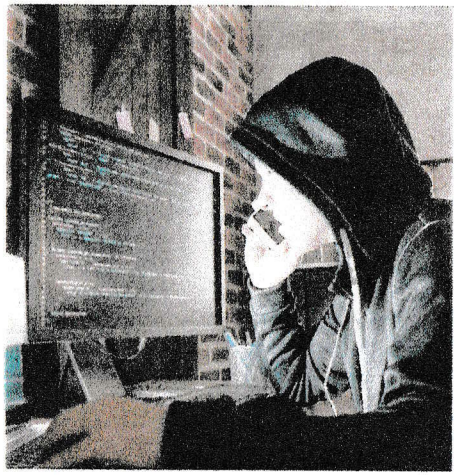
Aside from the usual busy evenings in Harrogate town centre with increased numbers enjoying the social scene, and the odd few spoiling it for the majority, I am pleased to say the festive season passed without significant or major issues to our communities in the Harrogate area.

Thank you for your part in this – it is essential we continue to look out for each other and be considerate of one another as we look ahead this year, where our attention has already turned to a range of community concerns and risks.

It is important now that I offer you advice about ever-increasing type of crime that presents a significant threat to us all, especially at this time of year – fraud.

Criminals look to take advantage of people of all ages who are enjoying the January sales and conducting financial transactions online. It is also known that fraudsters prey on individuals who have made New Year's resolutions to find love using dating websites.

There are also a whole host of dastardly telephone scams doing the rounds with the sole aim of extracting your cash by whatever means necessary, including making sickening threats to vulnerable and elderly people.



Don't be tricked into giving a fraudster your personal or financial details.

North Yorkshire Police is determined to tackle the ever-growing issue of personal fraud, so please take on board the following advice. For more information go to the North Yorkshire Police website www.northyorkshire.police.uk/fraud.

1. Requests to move money – A genuine bank or organisation will never contact you out of the blue to ask for your PIN, full password or to move money to another account. Only give out your personal or financial details to use a service that you have given your consent to, that you trust and that you are expecting to be contacted by.

2. Clicking on links/files – Don't be tricked into giving a fraudster access to your personal or financial details. Never automatically click on a link in an unexpected email or text.

3. Personal information – Always question uninvited approaches, in case it's fraudulent. Instead, contact the company directly using a known email or phone number.

4. Don't assume an email or phone call is authentic – Just because someone knows your basic details (such as your name and address or even your mother's maiden name), it doesn't mean they are genuine. Be mindful of who you trust – criminals may try and trick you into their confidence by telling you that you've been a victim of fraud. Criminals often use this to draw you into the conversation, to scare you into acting and revealing security details. Remember, criminals can also make any telephone number appear on your phone handset so even if you recognise it or it seems authentic, do not use it as verification they are genuine.

5. Don't be rushed or pressured into making a decision – Under no circumstances would a genuine bank or some other trusted organisation force you to make a financial transaction on the spot; they would never ask you to transfer money into another account for fraud reasons. Remember to stop and take time to carefully consider your actions. A genuine bank or some other trusted organisation won't rush you or mind waiting if you want time to think.

6. Listen to your instincts – If something feels wrong then it is usually right to question it. Criminals may lull you into a false sense of security when you are out and about or rely on your defences being down when you're in the comfort of your own home. They may appear trustworthy, but they may not be who they claim to be.

7. Stay in control – Have the confidence to refuse unusual requests for personal or financial information. It's easy to feel embarrassed when faced with unexpected or complex conversations. But it's okay to stop the discussion if you do not feel in control of it.

If you've taken all these steps and still feel uncomfortable or unsure about what you're being asked, never hesitate to contact your bank or financial service provider on a number you trust, such as the one listed on their website or on the back of your payment card.