Beware of COVID-19 related scams

It may seem unthinkable that people would attempt to profit from the Coronavirus outbreak. However, we're hearing stories that remind us that we all need to remain vigilant and aware of fraud risks, in both our work and home lives.

Every day, people and organisations are offering genuine support, and we all want to believe that everyone has good intentions and will 'do the right thing' to help those in difficult circumstances. Sadly, there have also been many reports of scams and an increasing number of fraudsters looking to take advantage of the current situation.

Here are a few scams to be aware of;

- **Online shopping**: High-demand items being offered such as hand sanitiser and PPE which are never delivered. Watch out especially for unsolicited messages offering questionably good deals.
- **Free school meals payments**: Text messages requiring that you provide your bank details in order to receive payments in lieu of free school meals whilst schools are closed. These may appear to be from Gov.UK. Please contact your school about FSM vouchers if you're uncertain.
- **COVID related fines**: Text messages indicating you have received a fine for leaving your home for non-essential purposes. Again these may appear to be from Gov.UK.
- **COVID related research**: Emails purporting to be from research groups or health organisations such as the World Health Organisation conducting surveys or offering access to data – these are phishing tactics used to gather your information, or may request donations.
- **Lender loan scams**: Taking advantage of people's financial concerns, these are (often unsolicited) offers of quick loans where you pay an up-front fee but the loan is never received.

•**Pension 'liberation' and investments**: As above, if financial hardship occurs, people may become more vulnerable to callers or mail offering great returns on their pension savings for an up-front fee or investment. The Pensions Advisory Service (PAS) offers lots of information and guidance about avoiding scam schemes.

•**Working from home: Computer service fraud**, including pop-up messages and emails offering service claiming to fix your slow IT systems. You should never install any software, or grant remote access to your computer, as a result of a cold call or pop-up. This should not be an issue on WBC equipment which has protections in place, but it is worth remaining vigilant and taking care on your home systems.

•**Working from home: Mandate fraud**, where you may receive fraudulent email which appears to be from a senior manager, or from a supplier, requesting that you change some payment details and make an urgent payment. These requests are taking advantage of colleagues and suppliers not being as readily available to speak to as they would normally be. If in any doubt, do not act until the request can be verified, directly with the manager or supplier.

Also, please be mindful of the following:

•**Volunteering**: Where you have volunteered to help in your community, be careful with your own and others' personal and financial information, bank details etc. You should find guidance to support you to volunteer safely, for example on Community Support Hub.

•**Staff unavailability/ changes to working practices**: We should be maintaining our pre-existing processes and controls, which help us to prevent fraud. However, reduced staff numbers, and inability to access the office, may result in some necessary changes to our processes, and we are working to ensure any changes are appropriate and properly communicated by managers, but if you are uncertain, you

should verify any requests to do things differently, particularly if this involves collecting, changing, or processing personal or financial information, ordering services, or making payments.

- **Emergency government measures** such as new grants and reliefs: Processes will be put in place to manage these, but you should remain vigilant to potentially fraudulent applications and/or identity theft.

If you have any concerns about potential fraud or scams, please contact Julie Gillhespey – Audit Manager, or Jen Brunning – Senior Auditor by emailing Julie.Gillhespey@westberks.gov.uk or jen.brunning1@westberks.gov.uk

(01635) 503206 | Ext 3206 |