More scams during the Coronavirus outbreak

Sadly, coronavirus related scams continue to rise as fraudsters seek to take advantage of uncertainty during this difficult period.

Information and advice about some scams is already available on the Buriton Community Website, here, but here are some reminders of common scams to be aware of, and advice on how to avoid them so as to stay safe.

Fraud – some basic tips

- You should never be contacted by anyone to ask you to log into your online bank account to check if you have received a refund, or to return an overpayment - Never tell ANYONE your online banking verification codes
- Never agree to download software or an app onto your device.
- You can contact a genuine company by using a trusted number from their website or, if it is your bank, use the number on the back of your card.

Impersonation Fraud

Fraudsters are using Coronavirus as a way of pretending to pose as genuine organisations that they know people look to for advice, such as banks, the police, government and even the World Health Organization (WHO). They'll use bogus emails, phone calls, text messages and even social media posts to try and get you to disclose your personal or financial information. Don't be pressured into doing something you're not sure about, any legitimate requests will allow you to check it out.

Health scams

Be wary of any texts or emails that look like they're from trusted sources, like the WHO who are asking you to open attachments or click on any links, as they may contain malware. Watch out for any advertising that promises to help combat or cure Coronavirus, from face masks to testing kits : if cures or help are available then it will be shared by the government or WHO. Remember, if it looks too good to be true, it usually is.

Official impersonations

Be vigilant to any 'out of the blue' contact either by text message or from a telephone call, especially those claiming to be from the police or fraud teams that ask you to move your money to another account. Trusted sources would never ask you to do this. Do not respond to any calls, emails or texts from companies saying that your computer or internet may be compromised. If somebody calls you, no matter who they say they are, it's important that you never agree to download an app or software on to your laptop, computer or mobile device. Especially if they then ask you to log in to your online banking accounts. Remember never tell ANYONE your online banking verification codes.

HM Revenues & Customs

Do not respond to any emails, calls or texts from HMRC saying you're owed a tax refund, or have an overdue tax bill. If you have any concerns contact HMRC directly, but not by using any of the links and the telephone numbers in the email.

Visitors to your home

Some fraudsters are even knocking on doors in some parts of the country claiming to be from local health authorities, trying to collect donations, or good Samaritans offering help. Remember that there is no door-to-door testing for Coronavirus and take extra care if someone is requesting personal information from you. If in doubt do not open your door.

Requests for support

Be careful if you receive any social media or text messages from what appears to be from friends or family asking for financial help during this time. Give them a call first to ensure the request is genuine.