Fraud Advice

Please be aware that during the Coronavirus crisis the fraudsters are trying to take advantage by sending malicious texts, emails and making phone calls. Please be careful and don't click on links within emails or texts if you aren't certain where they have come from. Fraudsters often use the logo of official organisations but neither HMRC or the Police will ask for payment or your bank details in this way. If you aren't absolutely certain if a link is a fraud or not please contact the organisation first by locating the telephone number independently yourself and not using one quoted on the message.

Action Fraud has this advice:

Do not give any personal information (name, address, bank details, email or phone number) to organisations or people before verifying their credentials.

Always question unsolicited calls, texts or emails requesting your personal or financial information (name, address, bank details, email or phone number). Instead, contact the company directly using a known email or phone number.

Many frauds start with a phishing email. Remember that banks and financial institutions will not send you an email asking you to click on a link and confirm your bank details. Do not trust such emails, even if they look genuine. You can always call your bank using the phone number on a genuine piece of correspondence, website (typed directly into the address bar) or the phone book to check if you're not sure.

- Never automatically click on a link in an unexpected email or text.

- Remember, email addresses and phone numbers can be spoofed, so don't use those as a means to verify that a message or call is authentic.

- The best way to get in touch with a company is to use a known email or phone number, such as the one on the back of your bank card.

There is some excellent advice specifically about Coronavirus related fraud on the Action Fraud website: https://www.actionfraud.police.uk/alert/coronavirus-related-fraud-reports-increase-by-400-in-march