Fraudulent HMRC emails, text messages and other scams

Due to several instances where our clients have informed us of both successful and unsuccessful attempts by fraudsters to steal money or personal information, we feel that it is necessary to ensure all of our clients are aware of the risks facing each individual in today's digital environment.

Internet scams and phishing attempts pose a significant risk to any individual who has an online presence. They may take the form of an email, text messages, phone calls and misleading websites. These forms of communication can often appear authentic, with fraudsters using official logos and email addresses that appear to be real.

They will also generally include a website, email or telephone number for you to proceed to or contact should you have any queries. You should never click onto a website or communicate through an email address or telephone number that is sent to you this way. This will in most cases be a fraudulent contact who will try to extract sensitive information from you.

Tax refund fraud
A recent report stated that HMRC is consistently the most abused government brand. It is important to remember that HMRC (or any other organisation) will never send notifications of a tax rebate or ask you to disclose personal or payment information by email or text message.

In the first instance, we would strongly encourage individuals to contact The Hutchinson Partnership if you suspect you have been the recipient of fraudulent communication relating to HMRC or your personal tax affairs. As your appointed tax agent, The Hutchinson Partnership will always work with you to collect your tax refund. No other organisations need to be involved. If you are scammed in relation to tax fraud, we may then suggest that you forward this information to HMRC's fraud team.

It is also important to be aware of other potential threats when online. Fraudsters work under many different forms, often pretending to be representatives from popular online service providers, including banks, PayPal, Amazon, iTunes, eBay and more. It is therefore imperative that if something appears even slightly out of the ordinary, you seek further advice.

Should you believe you are the recipient of any other online fraud, you should contact the individual service provider directly by using contact details you know to be correct. You should always ensure that you are accessing the genuine website and contact the service provider through their authentic communication channels. Online service providers will often have a 'contact us' page on their website.

We would also suggest the following best practice rules:

- Never click any links or download/click into attachments in suspicious emails, messages or other forms of communication.
- Do not give out private information such as bank details or passwords.
- Ensure that your computer's antivirus software is kept up to date.
- Mark any unwanted emails as spam/junk which will prevent similar emails appearing in your inbox in future.
- Supplier requests to make payments to a new bank account should be verified using contacts/contact details that you already know.
- If you are suspicious, ALWAYS check with the service provider whether the communication you are receiving is genuine.
- When contacting other service providers, ensure you are using the authentic communication channels and are going through the correct websites.

You can forward suspicious emails to HMRC's phishing team at phishing@hmrc.gsi.gov.uk and suspicious text messages to 60599. For further information, see HMRC's 'Phishing and scams' webpage (www.gov.uk/topic/dealing-with-hmrc/phishing-scams), where you can find information on how to report an issue, and how to recognise scams.