In the light of the increasing disruption seen by many of our clients as more and more staff work from home or are not able to be in work, we felt it appropriate to highlight that this is a time when fraudulent activity can increase and, as such, increased vigilance is appropriate over the coming weeks and months. Below are four examples of more common fraud types but if something doesn't look right or is out of what you would normally expect to see then please do take a second look.

Phishing E Mails with web site links - Fraudsters are sending out coronavirus-themed phishing emails to trick people into opening malicious attachments or revealing sensitive personal and financial details. Emails which purport to be from research organisations affiliated with the Centers for Disease Control and Prevention (CDC) and the World Health Organisation (WHO) contact potential victims over email. They claim to be able to provide the recipient with a list of coronavirus infected people in their area. In order to access this information, the victim needs to click on a link, which leads to a malicious website, or is asked to make a payment in Bitcoin.

Smishing is a security attack in which the user is tricked into downloading a Trojan horse, virus or other malware onto their cellular phone or other mobile device. SMiShing is short for "SMS phishing."

SMS phishing uses phone text messages to deliver the bait to induce people to divulge their personal information. Fraudsters can exploit and use this personal information to commit fraud. Common examples may involve a text which states that there is a problem with your bank account and ask you to call a phone number or visit a link.

Other messages may be from fraudsters pretending to be from your bank saying that personal information about you has been posted on the internet and asking you to visit a website. At present, as well as banks this can include government agencies such as tax office suggesting help around VAT payments / tax payments and to clink on a link etc.

Invoice Fraud - Fraudsters pose as a creditor or supplier and advise you their company's bank details have changed (due to a Coronavirus outbreak). The communication will ask you to make all future payments to a new sort code and account number. We have already seen an attempted payment redirection scam on Bankline which quoted Coronavirus as the reason why beneficiary bank details needed to be changed.

The Bankline customer in question trades regularly with a supplier in China, but were told the Chinese bank account was out of action because of the virus, and therefore funds needed to be sent to an account in the USA instead.

Bogus Boss payment requests - Bogus emails are sent to staff claiming to be from a senior member of staff within the organisation such as a Director, CEO or Chairman etc. requesting an urgent payment. They will often say that the payment is needed due to exceptional circumstances and needs to be carried out immediately.

With remote working increasingly common, there is an increased likelihood that spoof payments will be issued to staff members using Coronavirus as the purpose for the unusual payment.

Information provided by Natwest Bank