**Guarding Against Fraud during COVID-19**

With large numbers of employees now working remotely and most people generally conducting their daily business online, it’s been widely reported that cases of fraud or fraudulent attempts have substantially increased during the COVID-19 crisis.

This is especially the case with the recent CBILS, self-employed income support grants and the business grant support schemes. These provide the obvious lure of funds being paid directly into employers’ and individuals’ bank accounts and has seen immediate impersonation attempts by sophisticated fraudsters.

In addition, many finance teams are currently operating with reduced numbers meaning they may not be as well positioned to intercept fraudulent correspondence. Reduced numbers may also mean segregation of duties within teams may not be as separated as before, increasing the risk of both errors and fraudulent actions.

It’s therefore crucial at this time that businesses and their employees remain vigilant and guard against all risks.

We’ve set out below some of the most prevalent scams, other risks and preventative measures and simple steps that businesses may wish to consider during these uncertain times.

**Coronavirus Fraudulent Emails (Phishing)**

Fraudsters are sending out coronavirus-themed emails (and Whatsapp messages) to trick people into opening malicious attachments or revealing sensitive personal and financial details. Examples of this type of fraud in recent weeks have seen emails and Whatsapp messages purportedly sent by the Government, HMRC, the World Health Organisation and some charity organisations.

**Coronavirus Fraudulent Text Message (Smishing)**

Similar to the above, smishing uses phone text messages to deliver the bait to induce people to divulge their personal information.

Many of the recent scams claim to help business and individuals by unlocking Government funds. Fraudsters can exploit this and use the personal information to commit fraud.

**Invoice / Payment Redirection (Supplier or Employee Bank Impersonation)**

Fraudsters are posing as a creditor, supplier or employee and advising you that their bank details have changed (due to a Coronavirus outbreak). These communications may ask you to make all future payments to a new sort code and account number.

**Bogus Boss or Bank Staff Impersonation**

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

We also understand there have been attempts by fraudsters impersonating Bank staff.

**Investment, Loans and Other Opportunities Fraud**

With interest rates at an all-time low and financial insecurities at an all-time high, people with money to invest are also becoming targets with the above. In addition, businesses/people who desperately need capital at this time are also being targeted with the fraudulent promise of quick access to funds.

**Internal Fraud**

As people work remotely and staff members are being furloughed, the segregation of duties within operating finance teams requires careful consideration. This situation can give rise to risk of internal fraud around payments and financial reporting or failure to spot an external fraud attempt.

**Remote Working and Cybersecurity Fraud**

As more people work from home, fraudsters are capitalising on poor cybersecurity to commit fraud against businesses.

**General Preventative Steps**

Some simple steps for organisations and/or their employees to take at this time are set out below:

* Always take a moment to stop and think before clicking on links or calling numbers which risk being an impersonation of trusted organisations. If in doubt, confirm the position by contacting the relevant body using contact information available in the public domain or a reliable source.
* Ensure all staff have updated antivirus software installed on laptops and home computers.
* Review your IT Security Policy and ensure all staff are aware of policies and procedures. Consider engaging IT experts to review your policies and to carry-out security test audits.
* Review the segregation of duties within your finance team.
* Provide guidelines to your relevant finance team to reinforce existing policy and procedures and raise awareness over fraud matters.
* Implement additional verification checks and procedures before making payments.
* Implement additional checks and procedures before applying any changes to standing data.
* Be especially wary of new contacts or amended payment detail requests.
* Contact your bank immediately if you think you’ve fallen for a scam.

***A Time for Increased Vigilance***

To summarise, while the temptation may be to shift focus to pressing operational and other business and financial needs, employers should maintain robust internal controls and IT cybersecurity policies while employees are working remotely due to COVID-19.

Employers should also consider whether additional or modified internal controls are required to combat the challenges of the current working environment.

Engaging staff to be vigilant at all times is crucial - encouraging employees to question requests, double check records and be just a little paranoid are all critical in improving your overall cybersecurity.

Should you wish to discuss any of the above, please do not hesitate to get in touch.