Staying Vigilant about Financial Scams

Sadly, as we live and work through the Pandemic, cyber criminals remain active and we continue to hear of some distressing cases. Whilst we discussed this topic in our Summer magazine, we make no apologies about highlighting it again.

Financial scams look and sound legitimate, which is why it's easy to be tricked. We urge everyone to be on their guard and remain vigilant. If you are concerned about anything you receive by email or phone relating to your finances that you don't recognise or aren't expecting, please do not hesitate to contact us for advice.

Financial scams take many forms and could be about insurance policies, pensions transfers, or high-return investment opportunities, including investments in crypto assets. Scammers are sophisticated, opportunistic and will try many things.

The Financial Conduct Authority (FCA) has a website called SmartScam.

www.fca.org.uk/smartscam

This has been set up to help people who have any concerns regarding their finances or concerns about a firm that may have approached them about a perceived opportunity.

There is now a link on the website that specifically looks at scams linked to the virus. These include the following:

» Exploiting short-term financial concerns, scammers may ask you to hand over an upfront fee – usually between £25 and £450 – when applying for a loan or credit that you never get. This is known as loan fee fraud or advance fee fraud.

» 'Good cause' scams. This is where investment is sought for good causes such as the production of sanitiser, manufacture of personal protection equipment (PPE) or new drugs to treat coronavirus.

» Using the uncertainty around stock markets, scammers may advise you to invest or transfer existing investments into high return and high risk investments.

.

» Clone firms - firms must be authorised by the Financial Conduct Authority to sell, promote, or advise on the sale of insurance products. Some scammers will claim to represent authorised firms to appear genuine. In particular, be aware of life insurance firms that may be cloned.

» Scammers may contact you claiming to be from a Claims Management Company, insurance company or your credit card provider. They may say they can help you recuperate losses by submitting a claim, for the cost of a holiday or event such as a wedding cancelled due to coronavirus. They will ask you to send them some money or your bank details.

» Cold calls, emails, texts or WhatsApp messages stating that your bank is in trouble due to the coronavirus crisis and pushing you to transfer your money to a new bank with alternative banking details.

Further to these, we are aware of some people receiving phone messages from individuals claiming to represent Amazon, who have concerns that somebody is trying to scam their Amazon account. They normally then encourage you to download some software to your phone or computer which will then provide them with the information they require to scam you. Interestingly, Amazon themselves actually have a section on their website about such a situation, highlighting how seriously they are taking this.

With so much happening at present, it is important to remain vigilant and our advice remains the same.

» If you are unsure of anything about your finances, speak to your adviser.

» Don't do anything in haste. If in doubt, put the phone down or delete the email.

» Never provide any personal information such as a PIN or password.

» Ensure you use a strong password system.

Finally, help spread the message about scams. Feel free to pass on this advice about scams to others. Everyone is vulnerable and cyber criminals sadly are, and will remain, active. By being aware of the signs to look out for, you can reduce the risk of becoming a victim.