26th March 2020

Cyber Security - Spotting email scams linked to Covid-19

We would like to reassure our clients that we operate to the highest standards of Cyber-Security. However, it is a reality that cyber criminals are already preying on fears of Covid-19. These 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. They are also very likely to target the vulnerable so it is important to remain vigilant.

Our Communications

I want to make clear that you will never receive an email from us asking you to take action with your investments without first having discussed it with you fully and having provided you with a written recommendation detailing our rationale. **If you are in any doubt about the content of an email from us, please telephone your Adviser before acting.**

Likewise, we will never act upon an email from you requesting a change to your investments such as a withdrawal or encashment without first speaking directly with you, using the contact numbers that we hold for you on your file. When we contact you will recognise our office number, and our Adviser's voice, and if there is still any doubt then we can arrange an on-line meeting via a means such as Skype, where you can actually see the Adviser on your computer screen.

'Phishing' Emails

We are aware that scammers are sending 'phishing' emails that try and trick users into clicking on a bad link. Once clicked, the user is sent to a suspect website which could download malware onto your computer, or steal passwords. The scammers may claim to have a 'cure' for the virus, offer a financial reward, or be encouraging you to donate.

Like many phishing scams, these emails are preying on real-world concerns to try and trick people into doing the wrong thing. We suggest you refer to UK Government's National Cyber-Security Centre's guidance (https://www.ncsc.gov.uk) on dealing with suspicious emails to learn more about spotting and dealing with phishing emails.

What to do if you have already clicked on a link

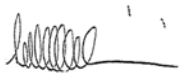
The most important thing to do is not to panic. There are number of practical steps you can take:

- Open your antivirus (AV) software if installed and run a full scan. Follow any instructions given
- If you've been tricked into providing your password, you should change your passwords on all your other accounts immediately
- If you're using a work device, contact your IT department and let them know
- If you have lost money, you need to report it as a crime to Action Fraud. You can do this by visiting actionfraud.police.uk

If you have any concerns, please contact your Adviser by telephone or email in the usual way.

Stay safe in these challenging times, we are here to help, and if you are in any doubt about the validity of any correspondence from us, whether via phone, email or letter, simply pick up the phone. You can find our telephone numbers and email contacts here.

Best regards,



Ian Wilkinson

Group Managing Director