Staying vigilant about Financial Scams

It is a distressing reality that even during the Covid-19 pandemic when so many people are themselves facing testing times, cyber criminals are still active. Financial scams are becoming more sophisticated. 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.

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 very important to remain vigilant.

These are some of the scams you should look out for:

'Phishing' Emails & 'Smishing' Texts

Scammers send 'phishing' emails or 'smishing' texts that try to trick users into clicking on a bad link or verifying account and password details. They often pose as someone official, such as your bank or building society, or even a Police Officer. Or they may claim to have a 'cure' for the virus, offer a financial reward or be encouraging you to donate.

Scammers can convincingly 'clone' email addresses to make their emails seem genuine – check the email address carefully.

Once you click on a link or reply by text, you are sent to a suspect website which could download malware onto your computer, or steal your passwords. This is actually a fraudster contacting you, who can read the information you type in.

These scams prey on real-world concerns to try and trick people into doing the wrong thing. Refer to the 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.

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 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 **www.actionfraud.police.uk.**

Boiler room schemes

These scams promise investors an impressive return but deliver nothing but a big loss. You get a call out of the blue offering you an investment opportunity with high returns. You will most likely be told that you must act fast and transfer your money straight away. It's common for victims to part with tens of thousands of pounds. The Financial Conduct Authority (FCA) doesn't authorise boiler room schemes, so if you hand over your cash, it might be the last you see of it.

Pension liberation schemes

Scammers are bombarding people aged 55+ with bogus investment opportunities to try to get hold of their pension savings. One of the most common scams since the pension freedoms were announced involves alleged investment opportunities abroad. Consumers have been offered free pension advice or investment opportunities by phone, text or email.

Low interest rates have tempted people to take extra risks, making them vulnerable to such fake investments. Fraudsters can approach you by post, email or phone. If you're offered a 'must-have' investment or a free pension review out of the blue, be wary. Also be concerned if you're warned that the deal is limited and you must act now. Decisions involving investments should not be made quickly or under pressure.

Homebuying fraud

Scammers can try and intercept cash transferred as a home deposit to a solicitor in the lead up to exchange and completion. A computer hacker monitors emails sent between a solicitor and client. When a house sale money transfer is about to be made, the fraudster emails the homebuyer pretending to be the solicitor and tells them the details of the law firm's bank account have changed. The unsuspecting homebuyer sends their cash to the new account, where the fraudsters withdraw it.

If you're buying a property, watch out for any emails about payments, such as a change in bank details at the last minute. Many victims are told that the account is being 'audited' and so another one must be used. Contact your solicitor if you're in any doubt.

Freebie scams

Seemingly 'free' or 'trial offers' for products are duping people out of millions of pounds a year. To get the freebies, you need to enter your card details – although you're told you won't be charged for the introductory period. In fact, this free trial scam means you are often signing up to an expensive monthly subscription that is very difficult to get out of. Once this type of billing is approved – known as 'continuous payment authorisation' - money can be taken without any further contact.

Be careful about handing over card details online. If you can't see any clear terms and conditions of what happens to your details before you enter them, step away.

Help spread the message about scams

Please 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.