How to help prevent personal finance fraud

There are so many reports of scams involving personal finance fraud nowadays it is difficult to keep up with them all. There is now even new terminology to define the various ways that people are targeted such as 'phishing', 'vishing' and 'smishing'. A recent survey suggested that more than four in ten people have needed to cancel credit or debit cards after falling victim to fraud in the last year.

So, what can you do to protect yourself?

Cybersecurity

Ensure that your home computer/laptop has the most up-to-date anti-virus and security software installed. Some browsers come with security features built in so make sure they are activated. Your bank may also offer additional security and advice so check their website for details.

If you shop online make sure you only use secure websites. When making a purchase look for the locked padlock or unbroken key symbol in your browser. Use secure payment methods such as PayPal or a credit card and never send payment directly to a bank account.

Passwords

Ensure that you create strong passwords which include a mixture of numbers, symbols and uppercase and lowercase letters. You should also use a different password for each internet account. If you find these hard to remember make sure that you keep a record of them in a safe place rather than in your wallet or next to your computer/device.

Email & Texts

Be extra vigilant if an email asks you to click on a link. Fraudsters use these to forward you to a website which gathers your personal details or to install malware onto your computer. They may also send you a text telling you to urgently call a number or visit a specific website to update your details. Be aware that your bank will never contact you via email or text for this information.

Telephone calls

If you receive a phone call from someone claiming to be from a legitimate company and that your computer is experiencing technical problems, they may be attempting remote access in order to hack your personal details. Hang up straight away. Never give your personal or bank details over the phone unless you made the call and the number came from a trusted source.

FFA UK's 'Take Five to Stop Fraud' campaign urges people to pause and think carefully before responding to any requests for information and not to be pressurised into making decisions. Trust your instincts and don't automatically assume that an email, text or phone call is authentic, even if it seems to come from a reliable source and seems genuine.

If you think you think you have been a victim of fraud you should contact your bank and Action Fraud (0300 123 2040/actionfraud.police.uk).

Published in the Wigan Observer – 11th July 2017