Simple things to do against fraud

Criminals are getting cleverer in ways to part you from your money. Many do not even need to leave the comfort of their home (which may be thousands of miles away) to carry out their crimes.

Fraud is defined as “Wrongful or criminal deception intended to result in financial or personal gain”.

Criminals can carry out fraud face-to-face, over the telephone, or via computers. Traditional Police methods can only effectively deal with the first method, and so it is to other authorities, service providers and companies to help us manage phone and computer-based crime. This is something that, on the whole, they do well and usually without the public even noticing. When a crime is committed it is often the result of the victim not taking enough care of their personal details – and it is so easy to be duped, as any victims will tell you.

But we, the public, can do so much to reduce the risks and to stop the attempted crime even getting going. There are some very easy things you can do.

Register with the Telephone Preference Service and the Mailing Preference Service. This stops UK companies cold-calling you or sending you junk mail.

If you get a telephone call from someone saying there is a problem with your computer or telephone then it is almost certainly a scam. Just ring-off – they don’t deserve the courtesy of a “no thank you”.

If your phone displays the caller’s number and it says “International” then it is almost certainly a cold-call and you should not answer (if you have friends or relatives abroad, programme their number into the phone so that you know it’s them calling). If you get an unexpected email from someone you know but with a suspicious text (or badly spelt) never click on any link in the email. The link is very likely to contain what is called a virus and is likely to load something into your computer that you really do not want in there. Whilst on subject of computers, buy an external disk drive and back up the computer at least once a week. Get a good anti-virus program loaded and make sure it gets regular updates. Many computers now come with anti-virus packages and so you do not even need to pay for it.

If you subscribe to social media (Facebook, etc) don’t post pictures of yourself on holiday as criminals can often find out where you live from your name and other details you may have on your account, and now they know your home may be empty because you are away. Make sure you put as few personal details as possible about yourself on social media.

If you have accounts with on-line companies, vary your passwords between them (having one password for each is never going to work as you’ll never remember which company has which password). Change the passwords at least one a year. If you need to make a note of a password use a “hint” that only you would know the answer to. Add capitals and special characters. Always “sign out” of websites when you leave them. Avoid registering your credit card details with companies – type it in every time. Consider paying with PayPal rather than directly to each company using your credit card.

All the above is based on common sense and is easy to do and costs nothing. But will considerably reduce the risk of fraud.