Scams, scams and more scams!

Fraudsters are always thinking up new ideas to separate people from their money. A few of the current scams are listed below.

1. Unsolicited phone call from someone, probably with an Indian accent, purporting to be from Microsoft and claiming there is a serious problem with your computer. You're asked to download a programme to get rid of a 'virus' and asked for personal information and bank account details. Best to put the phone down. Information about this and other Microsoft scams can be found at http://goo.gl/7tYlN.
2. A similar scam involves an unsolicited phone call from a company called 'TechAviators', telling you that your IP address or computer security has been compromised, and offering to fix the problem for a fee. The web is full of complaints about TechAviators. Again, the best response is to put the phone down, although it's tempting to play dumb and drag out the phone call. A recent warning by Cheshire Police relates to a company called Techfix that is operating a similar scam (see http://goo.gl/TssU6, item 6).
3. Yet another variant may ask you to give the scammer access to your computer to allow them to fix a problem! Don't even think about it! Best approach is to disallow Remote Assistance on your computer. For Windows XP go to Control Panel/System/Remote, then uncheck 'Remote Assistance' and (if it's there) 'Remote Desktop' checkboxes. For Windows Vista go to Control Panel/System/Remote Settings, uncheck 'Remote Assistance' checkbox and select 'Don't allow connections to this computer' option under 'Remote Desktop'.
4. An email, purportedly from HMRC, informs you that you are eligible to receive a tax refund, and asks you for personal details to allow the refund to be sent to your bank account. HMRC stresses that it doesn't send emails offering tax rebates and asking for bank details. Please report any such scam email to HMRC at phishing@hmrc.gsi.gov.uk. Email scams almost invariably contain grammatical and spelling mistakes, as illustrated by this amusing extract from an HMRC scam email.

> Please Click Here to have your tax refund to your bank account, your tax refund will be sent to your bank account in due time take your time to go through the bank we have on our list Note: A refund can be delayed a variety of reasons, for example submitting invalid records or applying after deadline.

5. Unsolicited letter, telephone or e-mail that offers the opportunity to invest money into things like shares, fine wine, gemstones, art or other 'rare' high value items, with the promise that they will rocket in value. What is offered is usually over-priced, very high risk and difficult to sell on, and may not even exist.
6. Official looking email purporting to be from Lloyds Bank, Natwest or similar, asks you to verify your account details. Those that have accounts with the bank in question may be fooled into clicking on to the link and giving their account details. No reputable bank would ever ask for personal details to be given via an email.

A few words of advice!

1. Don't respond to emails or calls of this nature. Put the phone down or delete the email.
2. Never give personal information or bank account details over the phone or by email.
3. Don't be seduced by the offer of an unexpected windfall. If an offer sounds too good to be true, it probably is!

Contacts for any issues relating to these scams are:

Police 0845-458-0000
Trading Standards 08454-040506
Crimestoppers 0800-555111

John Hammond 29/7/11