Do you know to whom you are answering the phone?

Telephone Fraudsters want access to your computer and your money (Computer Software Service frauds) – What is this and what can you do.

Telephone fraudsters are now cold calling/ making unsolicited phone calls pretending to be from your internet service provider, telling you there is a problem with your device or router, it could lead to fraudsters asking for credit card information to 'validate your software', or access to your computer to fix the problem. These are all scams, so what do you need to look out for.

Common scams that use the brand names include:

- Receiving a phone call from 'Microsoft Tech Support' to fix your computer.
- Receiving a phone call from your internet service provider i.e. BT, Sky, EE, Virgin etc.
- Receiving unsolicited emails with attached security updates.
- Being asked for your credit card information to 'validate your copy of Windows'.
- Being told you have won the 'Microsoft Lottery'.

They might say that they can fix the problem for a fee, or alternatively they can compensate you for the problem you are experiencing.
What these fraudsters really want is for you to unwittingly grant them remote access to your computer by installing software or visiting a particular website, and for you to give them your payment details. This is a scam.

These are all fraud scams - No reputable computer firm will send unsolicited emails or make unsolicited phone calls to request personal or financial information, or ask for access to your computer to fix it.

How to protect yourself

If you receive such communication delete the email or hang up the phone do not engage in a conversation. If you require further assurance contact the firm directly using the method and phone numbers obtained from their contract or other trusted sources, never use the numbers or email address supplied by the fraudsters.

- Legitimate companies like your Internet Service Provider (ISP), will never cold call you asking for remote access to your computer or for your financial details.
- Always be wary of unsolicited calls. If you're unsure of a caller's identity, hang up.
- Even if the caller is able to provide you with details such as your full name, don't give out any personal or financial information during a cold call however convincing they sound.

Never grant the caller remote access to your computer,
never go to a website they give you and never Install software as a result of the call.

- If you think you have downloaded a virus, consider having your computer looked at by a trusted technician in order to determine if malicious software was installed on your machine during the call.

Did you know that?

Fraudsters will keep your details so they can contact you again pretending to be a 'Recovery Company.' They usually advise victims that they can recover the lost amount for a small upfront fee.

- There are free services like the Telephone Preference Service (TPS) to block unsolicited calls.
- You can protect your friends and family (especially if you think they may be vulnerable) by telling them about the signs to watch out for.
- Having anti-virus software installed on your devices and keeping it up to date will help prevent your computer from being infected with malicious software.

ESSEX POLICE
Protecting and serving Essex

Report and get advice at:
www.actionfraud.police.uk
Other places for help and advice:
www.getsafeonline.org
www.cyberaware.gov.uk