Computer Software Service Fraud

What is computer software service fraud?

Fraudsters pretending to be from legitimate companies, such as your Internet Service Provider (ISP) or Microsoft, claim that they will fix your computer for a fee. They may cold call you to offer this "service", or create fraudulent websites, pop-ups and adverts in order to lure you into calling them. What they are really doing is attempting to obtain remote access to your computer and your financial details.

How to protect yourself from computer software service fraud:

- **Financial details:** Genuine organisations would never contact you out of the blue or ask for financial details such as your PIN or full banking password.
- **Installing software:** Never install any software, or grant remote access to your computer, as a result of a cold call.
- **Tech support:** If you need tech support, ask your friends or family for recommendations and look for reviews online first. Don't contact companies promoting tech support services via browser pop-ups.

What to do if you've been a victim of computer software service fraud:

- **If you have made a payment:** Inform your bank as soon as possible, they can help you prevent any further losses. Monitor your bank statements regularly for any unusual activity.
- **If you granted remote access to your computer:** Seek technical support to remove any unwanted software from your computer. Ask your friends or family for recommendations and look for reviews online first. Don't contact companies promoting tech support services via browser pop-ups.
- **You could be targeted again**: Fraudsters sometimes re-establish contact with previous victims claiming that they can help them recover lost money, this is just a secondary scam. Hang up on any callers that claim they can get your money back for you.

For more information on how to protect yourself from fraud and cyber crime, or to update your crime report, visit actionfraud.police.uk.