Computer software service fraud

FACT SHEET

How does computer software service fraud work?

Computer software service fraud occurs when fraudsters posing as legitimate companies, such as your internet service provider (ISP) or Microsoft, call to tell you that there's a problem with your computer.

They'll say something like:

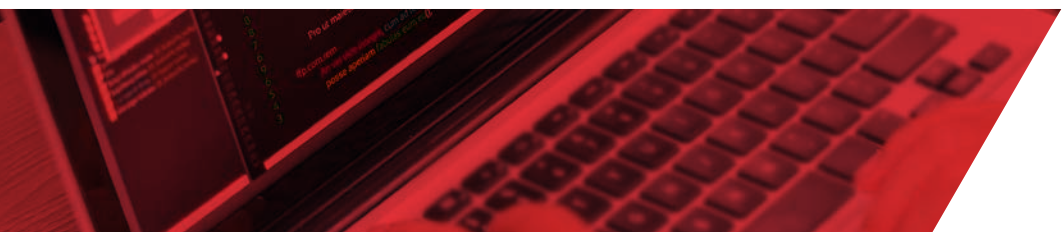
- there's a virus on your computer
- or there is something wrong with your computer
- or your router or internet connection are not performing properly

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.

What can be done about it?

- The majority of these frauds are carried out overseas through international call centres, so it is difficult for police in the UK to investigate. But something can be done. Reporting to Action Fraud enables intelligence to be gathered and preventative action to be taken by police. For example, suspending telephone numbers and websites used to commit this type of fraud.
- It is difficult for police to investigate every instance of fraud – prevention and protection is a far better method of dealing with it. By taking some simple steps, you can avoid falling victim in the future.



ActionFraud
National Fraud & Cyber Crime Reporting Centre
actionfraud.police.uk

Computer software service fraud

FACT SHEET

How to protect yourself

- Legitimate companies like Microsoft and Google 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. 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.

Report and get advice at:

www.actionfraud.police.uk

Other places for help and advice:

www.getsafeonline.org

www.cyberaware.gov.uk

ActionFraud

National Fraud & Cyber Crime Reporting Centre

actionfraud.police.uk