Spot the signs

Unsolicited calls	Software installation	Your information	Browser pop-ups
Unsolicited calls purporting to be from well known companies e.g. your Internet Service Provider [ISP] or Microsoft, offering to provide technical support for a fee	The caller instructs you to install certain software, or asks you to visit a particular website, so that they can gain remote access to your computer and 'fix' the problem	The caller may already know some of your details [full name or address] and use that to gain your confidence and extract further personal and financial information from you	Pop-ups purporting to be from well known companies e.g. your ISP or Microsoft, offering technical support and providing a number for you to call

How to protect yourself

Never reveal your personal or financial details as a result of a cold call	Never install any software or visit a website as a result of a cold call	Need professional support? Ask your friends or family for recommendations and look online for reviews first. Don't contact companies promoting tech support services via browser pop-ups

Report it to Action Fraud

If you have been a victim of Computer Software Service Fraud, report it to Action Fraud at actionfraud.police.uk
Even if you were able to recognise that it was a fraud and didn't lose any money, you should still report it to Action Fraud. Details such as the phone number you were called from, of the software or website they asked you to use, can help the police to disrupt criminal networks and arrest the individuals responsible.