Businesses Against Scams Fact Sheet

Tech support scams

With more people working remotely and IT systems under pressure, criminals may impersonate well-known companies and offer to repair devices.

How is the scam executed?

You receive a phone call or email offering to fix an issue such as a slow connection or software problem. You may be asked to make an advance payment, share login details or download software. Criminals are trying to gain access to your computer or get you to share passwords and login details.

Spot the signs

- Calls are often made from call centres so you may hear a lot of background noise, they will try and be your friend. 'I am here to help you'
- They may ask you to search an event log on your computer where warnings are in an attempt to validate the call or claim to be from your internet service provider and want to help you improve your internet speed
- A sense of panic will be created by using outlandish language like 'oh my god, I have never seen that many warnings before, please don't click on anything!'
- They will request payment to fix issues
- Once payment has been received, they may take it further and ask for access to your computer via a computer program, this is an attempt to harvest vital personal and company information on your computer

Stop, Challenge, Protect

If you receive a call out of the blue telling you that there is something wrong with your computer, stop and think, what are they asking for?

- Tech support companies do not send unsolicited email messages or make unsolicited phone calls to request personal or financial information, or to provide technical support to fix your computer
- Check with your manager which tech support company your business uses and initiate the call to them yourself using a number you know to be correct
  Report all suspicious communications to Action Fraud