



## Tech support scams – Fact Sheet

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

### How does it work?

You receive a phone call, email or pop-up advert 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

- **Background noise** - calls are often made from call centres
- **Professional** customer service: 'I am here to help you'
- Sense of panic created by using **exaggerated language** like 'oh my god, I have never seen that many warnings before, please don't click on anything!'
- **Request payment** to fix issues
- Ask for **access to your computer** to harvest 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.**

