scam share

spotlight on...

Remote Access Scams

Scammers frequently pose as IT companies, broadband providers or banks to try to trick people into allowing them to access their computer or other devices remotely.

what do remote access scam calls sound like?

The aim of these scam calls is to persuade you to give the scammer remote access to your computer or device, which could allow them to hack into your accounts or see sensitive data. Scam calls may say the following:

I'm calling from BT. We've detected that your router is not working efficiently and the speed can be improved. Please visit this secure website to download an upgrade...

I'm calling from Amazon Prime Security. Your account has been compromised and several payments have been made. Please download software which will allow me to access your computer and fix your account.

I'm calling from Microsoft Tech Support. There has been suspicious activity on your account - I'll need to access your device to fix the problem.

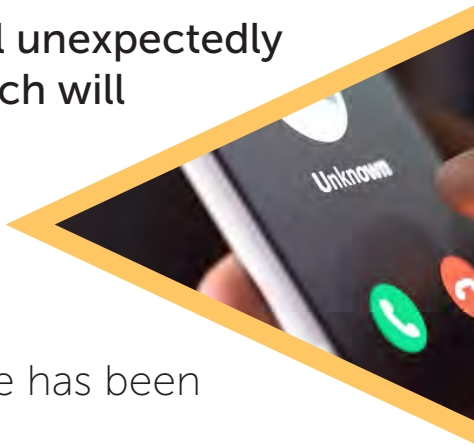
We have discovered a problem with your internet connection. Visit this website and download software which will allow us to access your computer remotely to perform tests and fix the connection.

I'm calling about the issues you've been having with your router. Download this app to your mobile phone so that I can check your broadband speed.

how can I tell if a call asking to access my computer is a scam?

Some of the companies which are most commonly impersonated by scammers are BT, Microsoft, Amazon and telecoms providers including SKY, Virgin Media and TalkTalk.

These companies have all stated that they will not call unexpectedly to ask you to install an app or download software which will allow them to access to your computer remotely.



These companies may need to remotely access your computer at times, but they will only do so if you have contacted them for support.

Scammers may try to scare you by telling you that there has been **"suspicious" or "illegal" activity** on your account.

Some scam calls may ask you to **download security updates** or new software by visiting a particular website - this could be used to download **viruses or malicious software** to your device.

what should I do if I get one of these calls?

Never follow instructions from an unsolicited caller to download an app or software which would allow them to access your computer remotely.

Never give any personal or account details to a cold caller.

If you are not sure whether a call is genuine, **hang up**. Clear the line and phone the company using a number found on a recent bill/statement or on their official website.

If you're worried that you have given a scammer access to your computer and that your details have been hacked, contact your bank immediately - they may be able to stop the money leaving your account. You should also report it to Police Scotland on 101.

Report all scams to **Advice Direct Scotland** using their free consumer helpline: **0808 164 6000** or via their website: **www.consumeradvice.scot**

Find more information and advice on avoiding scams:

Advice Direct Scotland - www.consumeradvice.scot
Police Scotland - www.scotland.police.uk/keep-safe
Trading Standards Scotland - www.tsscot.co.uk/latest-scams
The National Cyber Security Centre - www.ncsc.co.uk

Trading Standards Scotland