

scam

share

Remote Access Scams

spotlight on...



Scam calls where the caller poses as staff from an IT company, broadband provider or bank.

The aim of these calls is to convince people to allow the caller to access their computer or device remotely. This could let them hack into accounts or see sensitive data.

Common Scams



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

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 about the issues you've been having with your internet connection. Visit this website and download software which will allow me to access your computer remotely to perform tests and fix the connection...



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...



Avoid Remote Access Scams

-  **Never follow instructions from an unsolicited caller to download an app or software which would allow them to access your device remotely**
This could allow them access to any personal and banking details stored on the device
-  **Companies such as BT, Microsoft, Amazon and major telecoms providers 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 your device 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
-  **Don't give a cold caller any personal information or bank details, even if they have some details already**
If you are unsure about the identity of a cold caller, hang up and contact the company using details found on their official website or on a recent statement/bill
-  **Report remote access scams**
Report all scams to Advice Direct Scotland on 0808 164 6000 or via scamwatch.scot
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.

Find out more:

www.tsscot.co.uk/scamshare

