



# Remote access scams



Remote access scams attempt to gain access to your computer or personal devices by pretending to be from large, well-known organisations across all sectors including telecommunications, financial institutions, IT support and online retail. They may claim they've detected a problem which requires you to download additional software or to grant remote access to your devices. Once the scammer gains access to your device, they can see what's on your screen, access your files and even take control from you.

## How to spot a remote access scam

- You receive an unsolicited call from a trusted third party organisation.
- The caller claims there are technical issues with your computer or personal devices, or that a cyber attack has been detected.
- The caller asks you to download or purchase new software to protect your device.
- You're asked to disclose personal or banking information over the phone (by rule of thumb, legitimate companies won't ask this of you).
- The caller tells you they are sending you a verification code and asks you to read it back to them.
- The caller is persistent and may become threatening.
- Poor spelling or grammar in the communications and links that the caller sends to you.

## How to protect yourself

- Never give remote access to your device by clicking a pop-up, downloading an application or following verbal instructions.
- Never share your personal or banking information, including your credit card number or online account details over the phone unless you made the call to a trusted source.
- Change your Online Banking passwords often and don't use the same password for other accounts or systems.
- Take steps to strengthen your account security by setting up multifactor authentication and updating your device.
- Make sure your computer is protected by anti-virus software you have researched and installed yourself. Ensure you purchase software from a trusted source.

Scams continue to evolve and grow more sophisticated in their attempts to gain personal, banking information or access to devices.

### Stop

Say no, hang up or delete suspicious messages. Take your time, trust your instincts and avoid giving out any personal information or money if you're unsure.

### Check

Ensure the person you're dealing with is real. Contact organisations directly using contact details you find yourself. Verify investment offers through ASIC and confirm with family, friends or a professional before acting.

### Protect

Act quickly if you're concerned you've been in contact with a scammer. Contact us immediately and help others by reporting scams to Scamwatch ([www.scamwatch.gov.au](http://www.scamwatch.gov.au)) or the police ([www.cyber.gov.au](http://www.cyber.gov.au)).

**People First Bank will never contact you to request your passwords, VISA card or account details.**

We will not send you SMS containing links. Never share your password or Online Banking login credentials.

If you have been contacted or are concerned about your privacy, please call us directly on **13 11 82** or visit a branch.