

Staying Safe Online – **REMOTE ACCESS SCAM**



STOP.
THINK.
CHALLENGE.

Be on guard for scammers who contact you claiming they need access to your computer to fix an issue.

How this scam works:

Scammers will try to trick you into believing that they work for a familiar company, like a telecommunications company, an IT company or a bank. They will sound professional and give you a fake but believable story about needing access to your computer or device to fix a problem.

They will claim that there is an issue with one of your services, like your internet connection, or your phone line, which is affecting your computer's performance. They may say your computer is now sending error messages, or that it has a virus, or it has been hacked.

The scammer will say they need to access to your computer remotely to find out what the problem is, or to fix it. They might also ask you to download an App to your device claiming it will help them fix the issue. This App contains software, called malware, which provides access for the scammer to your passwords and potentially other personal information.

3 warning signs

- 1** You receive a phone call out of the blue and the caller claims to be from a large telecommunications or computer company, or a technical support service provider. They say that your computer is having technical problems and they need remote access to sort it out for you.
- 2** You are asked to buy software or sign up to a service to fix the computer. Your personal details and your bank or credit card details are also requested.
- 3** The caller is very persistent and may become abusive.


3 ways to protect yourself

- 1** If you receive a phone call out of the blue about your computer and remote access is requested – hang up – even if they mention a well-known company such as Telstra. Telstra does not request credit card details over the phone to fix computer or telephone problems, and is not affiliated with any companies that do.
- 2** Never give an unsolicited caller remote access to your computer. Never provide your personal, credit card or online account details over the phone - unless you made the call and you're **certain** you called the correct phone number.
- 3** Remember that you can still receive scam calls even if you have a private number or have listed your number on the Australian Government's Do Not Call Register. Scammers can obtain your number fraudulently.



Hang up if you receive a phone call out of the blue requesting remote access to fix problems with your computer.

Think you've been scammed?

 If you think you have been a victim of a scam it's important to call **Heritage on 13 14 22 (available 24/7)** promptly to limit any further loss and to see if the transactions can be reversed or disputed. If you are overseas please call +61 7 4694 9000.



Go to our website to download more information about scams:
www.heritage.com.au/scams

DO NOT make further payments to the scammer.

Please ensure you change your passwords to secure your account and report the scam to [ACCC \(www.accc.gov.au\)](http://www.accc.gov.au) via the report a scam page. For more information on how to protect yourself from scam visit the [Scamwatch website \(www.scamwatch.gov.au\)](http://www.scamwatch.gov.au).

Heritage Bank
People first.