

Introduction

What is a remote access scam?

A remote access scam is when a scammer convinces people to give them control of their computer, phone, or tablet using forms of manipulation designed to increase stress or urgency.

How do remote access scams happen?

Remote access scams often start with an unexpected phone call, text message, pop-up alert, fake IT support, or online advertisement. The scammer may ask you to download remote access software or follow steps to allow them to control your device. Once they have access, they may steal information, monitor your activity, or manipulate what you see on your screen.

Prevention

How can I tell when a request for remote access is not legitimate?

It is important to note that remote access tools are legitimate programs commonly used for IT support and remote work. However, criminals are well-known to abuse these tools to conduct fraud while posing as legitimate services. The below checklist can help you to identify if a request for remote access is legitimate.

- ☐ The request was initiated by an unexpected call claiming to be from a telco, utility provider, your bank or a Government agency.
- ☐ The caller claims your IP address is compromised, your internet is slow, or that criminals may soon access your financial accounts if you do not act swiftly.
- ☐ The request originated from an investment advisor or stock trading broker who wishes to show you how to trade or use related tools in relation to an online enquiry you recently made about an investment.
- ☐ A pop-up alert or advertisement that claims your device is infected or compromised and provides a number to call to fix the issue.
- ☐ The request includes pressure to act immediately, stay on the call, or keep the conversation secret.
- ☐ While remotely viewing your screen, you are asked to log in to online banking or other online accounts to ensure they have not been hacked or compromised.

Sharing & Disclaimer

IDCARE is a not-for-profit and registered Australian charity.

© Copyright Identity Care Australia & New Zealand Ltd. While every effort has been made to ensure the accuracy of the information in this document, IDCARE disclaims any liability to any person with respect to any actions performed or not performed as a result of the contents of this document.

Detection

How can I tell if I have already provided remote access to my device?

Again, the presence of remote access software on your device does not immediately indicate you are a victim of a scam. You may have previously provided access to your device via a legitimate pathway – which could include when you engaged support from I.T services via your workplace or school or have paid for a premium technical support service through an existing provider. The important distinction is that legitimate requests will be subscription based, pre-arranged and will occur after you have contacted the provider yourself. They will also be focussed on technical assistance and not moving money or securing accounts in response to alleged crimes. A legitimate service will never pressure you to act.

- ☐ While using your device, your cursor (mouse) moves or clicks on its own.
- ☐ Apps and files open without your input.
- ☐ Your screen changes or settings are modified unexpectedly.
- ☐ You remember downloading a program or app, and entered a code or clicked 'accept' to a "connection request" or "remote session" through this program or app.
- ☐ You can see one of the below icons on your device:



Sharing & Disclaimer

IDCARE is a not-for-profit and registered Australian charity.

© Copyright Identity Care Australia & New Zealand Ltd. While every effort has been made to ensure the accuracy of the information in this document, IDCARE disclaims any liability to any person with respect to any actions performed or not performed as a result of the contents of this document.

Response

What do I do if I have provided remote access to my device?

1. Disconnect from the internet

- ☐ Turn off Wi-Fi, unplug the internet cable, or switch on airplane mode to stop the remote connection.

2. Stop communicating with the scammer

- ☐ Hang up the call and do not respond to further messages. Scammers may pressure or threaten you to keep you engaged.

3. Contact your financial institution

- ☐ If your device was accessed, contact your bank immediately. Assume any information stored on the device may have been viewed or accessible.

4. Change your passwords

- ☐ If possible, use a different, trusted device to change passwords for your banking, email, social media, and other important accounts. Also update any passwords saved in your browser or stored in documents.

For additional support or information, contact IDCARE:

Submit [Get Help Form](#) | 1800 595 160 (Aus) | 0800 121 068 (NZ)

Sharing & Disclaimer

IDCARE is a not-for-profit and registered Australian charity.

© Copyright Identity Care Australia & New Zealand Ltd. While every effort has been made to ensure the accuracy of the information in this document, IDCARE disclaims any liability to any person with respect to any actions performed or not performed as a result of the contents of this document.