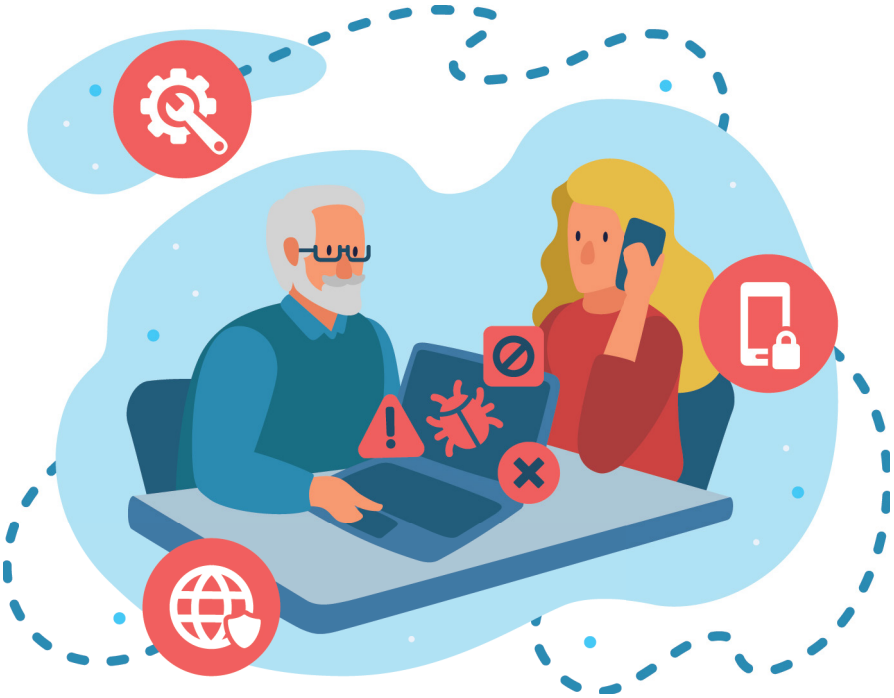
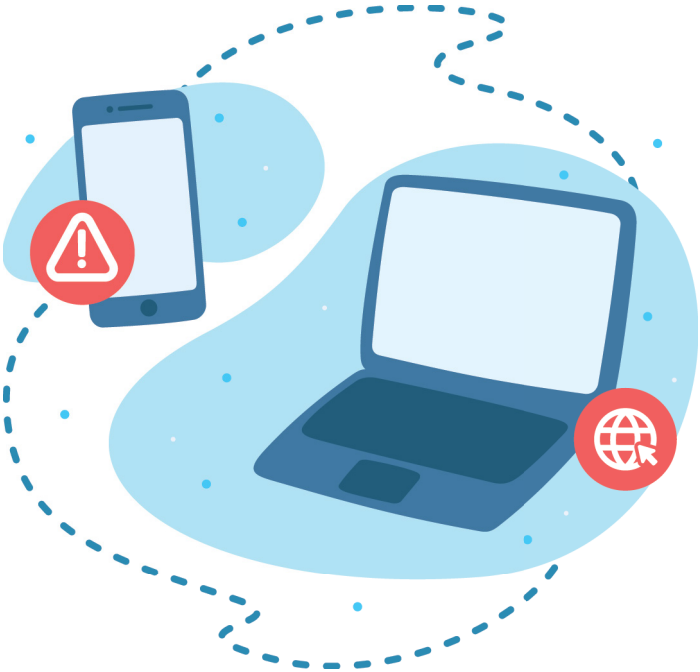
Your Digital Safety Guide

Avoiding Phone and Internet Scams



accan

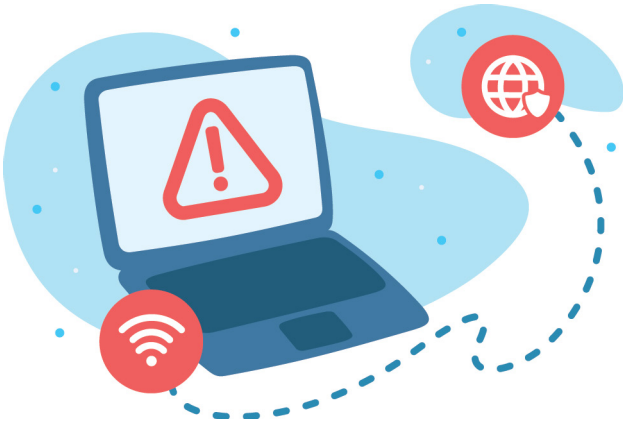
Scammers are constantly changing the ways they work and adapting to new technologies. To keep yourself safe, it's important to know how scammers can use phones and the internet to try to profit from your personal information.



Types of Scams

Technical Support Scams

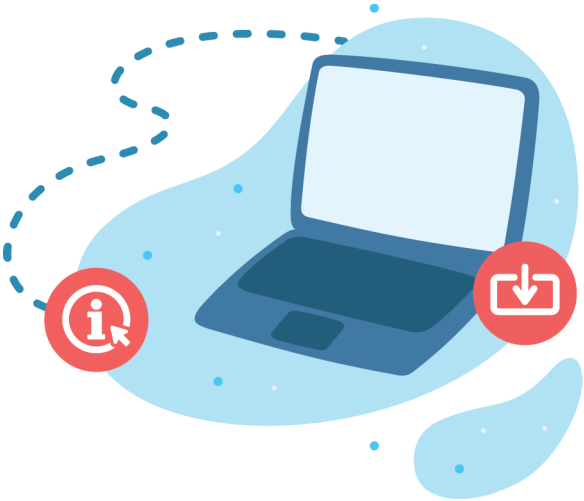
This type of scam usually uses telephone cold-calls, browser pop-up window or paid search results on search engines like Google to trick people into thinking that there is malware or a virus on their computer.



Technical support scammers will often try to get you to install a remote access program that lets them control your computer.

Scammers will lie, saying that this is done to help solve the computer's issues. However, letting them into your computer will only cause more problems as they can access your personal information, documents and install malicious malware.

If granted access to your computer, the scammer may also claim that they have found the problem with your computer and ask you to pay a fee to fix it.



Phishing Scams

Scammers can send you messages where they pretend to be from a company or organisation that you trust (such as your telco, your bank or a Government agency like the Australian Tax Office). These messages can be sent as emails, SMS messages, or through social media.

Phishing messages often ask you to click a link and enter your personal details.

Be aware that legitimate companies will not call, text or email you to ask you to update or verify your password, PIN, account details or credit card information. They will also not cold-call you to request payments over the phone.

Before you click a link (in an email or on social media, instant messages, other webpages, or other means), hover over that link to see the actual web address it will take you to (usually shown at the bottom of the screen). If you do not recognise or trust the address, try searching for relevant key terms in a web browser. This way you can find the article, video, or webpage without directly clicking on the suspicious link.

Missed Call Scams

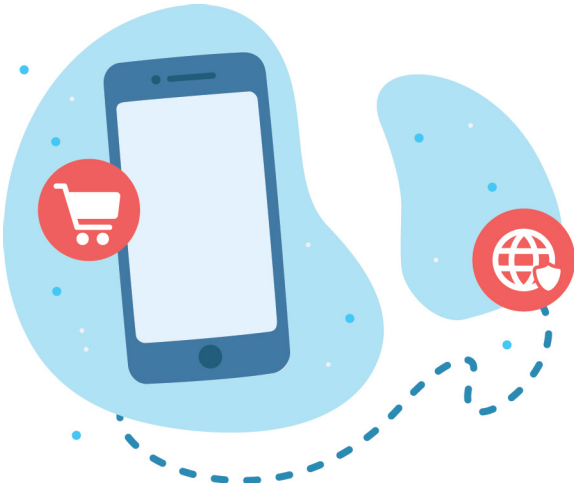
These scams work by making a very short call to your mobile phone before hanging up. Scammers want you to call back the missed number so that they can charge you at a premium rate. The longer that they can keep you on the phone, the more money they can make from you.

If you don't recognise the number, if it is an international number, or the phone number starts with 1900 (which identifies a premium rate service), there's a chance that it may be a missed call scam.

Fake Online Shopping Scams

Online shopping scams involve scammers pretending to be genuine online stores. This is usually done with a fake website that closely resembles the real deal (e.g. using a capital “i” to replace the “l” in “Telstra.com.au”), or by setting up a website that doesn’t deliver goods as promised.

Many of these online shopping scams aim to take your money, while others use your personal information for identify fraud.



Avoid fake online shopping websites by staying away from stores that advertise products at unbelievably low prices (e.g. selling the latest iPhone for $100).

When making payments online, you should also look for secure websites – these have a closed padlock symbol in the URL bar and begin with “https”.

How to Stay Protected from Phone and Internet Scams

- Never let strangers remotely access your computer, even if they claim to be from a well-known company.

- If you're not sure that a call is legitimate, hang up and call the company back by using their official contact details.

- Don't call back phone numbers that start with 1900, or unknown international numbers.

- Don’t click on links in emails or messages, or open attachments, from people or organisations you don’t know.

- Be careful about how much personal information you share on social media sites.

- Regularly update your computer with anti-virus and anti-spyware software.

Getting Help for Scams

The Australian Competition and Consumer Commission (ACCC) runs the SCAMwatch website, which contains information about different types of scams, and what you can do if you think you have been scammed.

You can also report scams to the Australian Cyber Security Centre (ACSC).

Many banks, phone companies and other service providers include information on their websites about how to detect and avoid scams.

Contact Us

Website: accan.org.au

Twitter: @ACCAN_AU

Facebook: facebook.com/accanau

E-mail: info@accan.org.au

Phone: 02 9288 4000

For more information and tips go to:
accan.org.au/tips

Australian Communications
Consumer Action Network