Protect against scams

Top tips

Scams are something everyone should be aware of. Phone calls, emails, text messages, posts, tweets, websites and even online ads may all be used to scam.

And while scams may take many forms, they are all alike in their aim – to steal or cheat you out of money or information. A few common sense steps will make you very difficult to scam!

1. Be a little suspicious

Unusual or unexpected emails, messages or calls, and particularly those seeking money or personal information, should make you suspicious. Your suspicion is useful!

2. If you're not sure the message or person calling is legitimate, check them out before you respond

If you're suspicious about anything, there's action you can take. Find out if the message really is from that organisation by independently checking with an organisation's website or call them on their official advertised phone number.

3. Be selective about disclosing your personal information

Just because they're asking for it, doesn't mean they need it. Minimise what you disclose and where you disclose it. Never reveal your password or other sensitive information such as your date of birth or tax file number.

Learn to identify and avoid scams and phishing*

Develop your sense for what might be a scam. Unsolicited contact seeking your money or your personal information, regardless of the reason, should immediately trigger suspicion. Many organisations provide examples of current scams on their websites. You can also check the Australian Government's SCAMwatch radar for known scams scamwatch.gov.au.

Phishing* emails range from looking very authentic to being poorly written including spelling mistakes

They will OFTEN contain a link or an attachment designed to entice you into clicking on it. Sometimes they will simply look to elicit a response or ask for personal info or account details.

Don't respond, open attachments or click links in suspicious texts, posts, emails or tweets. Delete them

Scammers attempt to reach out to you in many different ways, but you can avoid most scams easily by not clicking on the links or attachments. If something makes you suspicious or doesn't look quite right, avoid opening it. Simply delete it and move on.

Stay with trusted websites and mobile applications (apps)

Conduct your activities with websites and apps you trust. Well known, reputable organisations are more likely to have secure websites. Put the websites you use most often into your 'favourites' list. Avoid websites or software, including mobile apps, unless you are confident they are safe and reliable. Only download apps from trusted or official sources (i.e. Google Play Store on Android etc)

Check website addresses are written correctly, and look for a secure 'https' connection for pages where you're entering sensitive data

Scams often impersonate legitimate websites. The 's' in an 'https' page address indicates your connection is secure – critical for protecting your information or transactions. Most internet browsers will also display a small padlock in the address bar. Navigate to banking websites yourself, don't click links in messages.

Be wary of pop-ups and 'notifications' which can feature scams and dangerous links

Pop-ups (small internet browser windows that automatically pop up on your screen while you visit a website) can contain malicious links, ads and requests for information. Avoid clicking on these. Many browsers have built in pop-up blockers which you should enable.

What is phishing?

*Fake or deceiving electronic messages (e.g. emails or texts) used to elicit a response such as revealing your personal, financial or account information to a scammer