

TPB on scams awareness

The Tax Practitioner's Board (TPB) has advised that the number one way to prevent scams is by talking about them with family, friends, colleagues and clients to spread awareness, in line with the theme of this year's Scams Awareness Week. Scams cost Australian consumers, businesses and the economy hundreds of millions of dollars each year and cause serious emotional harm to victims and their families.

As at 31 August 2021, Scamwatch received over 190,000 reports with losses over \$192 million so far this year. This is a 95.4% increase in losses since this time last year. Investment scams cause the most financial loss in Australia, with over \$96 million having been lost so far this year. Cryptocurrency scams are the most popular type of investment scams, representing over 50% of losses. Often the initial investment amount is low (between \$250 and \$500) but the scammers pressure the person to invest more over time before claiming the money is gone or ceasing communication and blocking access to the funds. All age groups are losing money to investment scams, but the over 65s have lost the most with \$24 million lost.

The TPB says talking about scams removes stigma, spreads awareness and can also help people get out of them sooner rather than later if they are already in one. It says some other simple steps that can be taken to protect individuals and their businesses are:

- Never giving any personal information to someone who has contacted you.
- Not clicking on hyperlinks in text/social media messages or emails, even if it appears to come from a trusted source.
- Going directly to a website through your browser. For example, to reach the MyGov website type "my.gov.au" into your browser.
- Never responding to unsolicited messages and calls that ask for personal or financial details, even if they claim to be from a reputable organisation or government authority — just press delete or hang up.
- Never providing a stranger remote access to your computer, even if they claim to be from a telco company such as Telstra or the NBN Co.
- To verify the legitimacy of a contact, finding them through an independent source such as an online search or past bill.
- Hanging up and verifying the identity of the person contacting you by calling the relevant organisation directly find them through an independent source such as a past bill or online search.
- Searching for reviews before purchasing from unfamiliar online traders.
- Being wary of sellers requesting unusual payment methods such as upfront payment via money order, wire transfer, international funds transfer, preloaded card or electronic currency, like Bitcoin.
- Verifying any request to change bank details by contacting the supplier directly using trusted contact details you have previously used.
- Considering a multi-factor approval process for transactions over a certain dollar amount.
- Keeping the security on your network and devices up-to-date, and having a good firewall to protect your data.

Where to get help

- Refer to [Scamwatch](#) if you or someone you know has been scammed, even if you didn't fall for it.
- If you believe you might have unwittingly shared sensitive information, divulged yours or your client's TFN or experienced a data breach, phone the ATO on 1800 467 033.
- If you are ever unsure about a request for information or the validity of an interaction by the ATO, call the ATO Scam Hotline on 1800 008 540 or visit the [ATO scam site](#).