



DON'T GET SCAMMED

THERE'S NOTHING QUITE LIKE DREAMING OF WHAT YOU'D DO IF YOU WON THE LOTTERY, OR IF A GOLDEN OPPORTUNITY TO MAKE SOME QUICK CASH SUDDENLY LANDED IN YOUR LAP.

It's nice to dream but unfortunately most of the golden opportunities that arrive in your email or your letterbox aren't designed to pay for your new Ferrari or a world cruise. More likely they are clever ways for criminals to siphon money out of your bank account before you realise you've been conned.

The extent and cost of consumer fraud to Australia is difficult to quantify, although it is clear that many consumers who get scammed can lose tens of thousands of dollars and the number of scam emails, phone calls and letters continues to rise.

A group of 18 government agencies in Australia and New Zealand have joined together to form a taskforce to inform and protect consumers from such rip-offs.

The Australasian Consumer Fraud Taskforce launched a Scams Awareness Month (ScAM) which runs from mid-February until mid-March and is designed to educate consumers about scams and how to guard against them.

The key message of the campaign is 'If a scam comes calling—destroy it, delete it or hang up!' and urges consumers to recognise scams and not to respond to them. ScAM will focus on four of the most common types of scam in Australia, most of which require some element of consumer participation to succeed—so the ACFT wants the 'do not respond' message to come across loud and clear.

While there are many different types of scams, thankfully there are a few basic steps all consumers can take to protect themselves.

Destroy! delete! hang up!

One of the first clues that an offer might be a rip-off is its source of origin. A good example is the email that arrives in your in-box informing you that you've won a lottery you never entered. These scams often rely on the recipient sending in a small 'administration fee' of, say, \$50. However, requests for more money keep on coming in, and consumers never receive their 'winnings'—some consumers have lost over \$10 000 to these types of scam!.

One of the most well-known types of scam is the Nigerian letter fraud, when you receive a letter from a government official or 'businessman' in an underprivileged country (originally many of these letters originated in Nigeria—hence 'Nigerian scam') asking you to use your bank account to help them launder some money out of their country, in exchange for a percentage of that money. The only thing that happens? Your bank account is wiped out and a stranger profits from your loss.

While it's often tempting to respond to annoying emails and letters, the best response is to destroy the letter or email without responding and if it's a phone call to hang up before you reveal any personal details.

Something smells a little phishy?

The increasing popularity of on-line banking has made it even easier for scammers to rip off the unsuspecting. It has given rise to phishing, a scam where a bogus email, usually disguised to appear as if it has come from a customer's bank, asks customers to confirm their personal details such as an account number or PIN.

It might include a convincing looking, but fake, form for you to fill out. Just remember that a bank will never ask its customers to confirm their account and PIN details in an email.

The advice from the taskforce is that consumers should immediately delete emailed requests for personal and financial details and certainly never follow the link if attached.

If you aren't sure about something, call your bank and confirm the email is in fact legitimate; ask questions and seek further information. Most importantly—DO NOT RESPOND! Just remember, no matter how sophisticated the scam, you can't be ripped off if you refuse to take part in it.

Want more information?

The ACCC's webpage ScamWatch will serve as the campaign's information portal, which will raise consumer awareness not only of the campaign and its message, but also of the ScamWatch website for their future reference. ScamWatch will be updated regularly throughout ScAM, with victim scenarios and explanations of different scams. If you or someone you know has been scammed, please call the scam infoline on 1300 795 995 or visit www.scamwatch.gov.au to report it.