How to recognise a scam

The trusty mobile phone opens up a world of information to us, and unfortunately vast opportunities for scammers. Perpetrators seek personal information like usernames, passwords, bank details, and more.

It often happens as innocently as this: it's Sunday morning and you're scrolling through your emails. As a regular PayPal user, your eyes are used to scanning for these emails. You open the email. The email address looks trustworthy, as does the communications inside that informs you that you need to log in. You've clicked on the link and typed in your password. Before you know it, a scammer has captured your password and all your financial and personal details. You've been scammed, and all within 20 seconds.

How to protect yourself from your inbox

There's a number ways to spot a scam email, here's what to look for.

- **Think before you click:** it's easy to mindlessly scroll through emails and clicking aimlessly on different links. Be suspicious of any links and attachments that you come across.
- **Copy and paste the email into Google**: This is a great tip! If in doubt, do an internet search on the exact wording of the message. It's likely it's a well-known scam that someone has already tried to warn others about.
- **Read it thoroughly**: Check that the email uses your proper name, is free of typos, and is being sent from a legit company email. Often scammer PayPal emails will come from an email that has extra bullet points, or strange letters. Be vigilant and check.
- **Make sure the website is secure**: good websites will have "https" in the web address and show the icon of a closed padlock at the start of the URL. Make sure you also check the domain URL. Scammers will have a website that looks similar, with a slightly sketchy web address.

Keep vigilant and wary on your next call from a stranger, and hyper-aware when browsing through your inbox.