Staying Safe Online – IMPERSONATION SCAMS

Scammers will try to trick you into believing that they are from a familiar organisation, and it often doesn't seem unusual they would be trying to contact you.

How this scam works:

Scammers will give you a fake but believable story about a problem with your bank account, a regular payment, a government benefit, or a fine that might need paying.

These scams often start with a phone call, text message or email that seems to be from a trusted organisation. You're convinced to make a payment or give personal and financial details to someone who says they are from an organisation you trust.

The scammers will use tactics to make their calls or text messages appear genuine by cloning an organisation's number or sending ID which is displayed on your phone. In some cases criminals even trick you by sending couriers to collect your cards, PINs or valuable items in person.

These scams are based on threats and intimidation tactics, so you should report any concerns immediately to the police and your bank.

3 warning signs

1. **You receive a phone call, text message or email out of the blue asking for your personal and/or financial information, to make a payment or move money.**
2. **You're told to act immediately, sometimes with the claim that "your money is at risk" or "your account will be blocked" or "there are suspicious transactions on your account". You are told that if you don't act immediately, you could be arrested or lose all of your money.**
3. **The sender's email address is similar, but ever so slightly different to that of the genuine organisation.**

3 ways to protect yourself

1. Never give your personal, credit card or online account details over the phone unless you made the call and the phone number came from a trusted source – like the organisation's official website.
2. If you receive a phone call out of the blue about your bank account, government benefit or a tax debt – hang up – even if they mention a well-known organisation such as Heritage, Telstra or the ATO. Locate the official contact number, often available on their website, and call them directly to verify they called you. Never use the contact details from the initial call.
3. Remember that you can still receive scam calls even if you have a private number or have listed your number on the Australian Government's Do Not Call Register. Scammers can obtain your number fraudulently.

Be on guard. Double check requests that seem legitimate from organisations you know.

Think you've been scammed?

If you think you have been a victim of a scam it's important to call **Heritage on 13 14 22 (available 24/7)** promptly to limit any further loss and to see if the transactions can be reversed or disputed. If you are overseas please call +61 7 4694 9000.

DO NOT make further payments to the scammer.

Please ensure you change your passwords to secure your account and report the scam to ACCC (www.accc.gov.au) via the report a scam page. For more information on how to protect yourself from scam visit the Scamwatch website (www.scamwatch.gov.au).

Go to our website for more information about scams: www.heritage.com.au/scams

Heritage Bank
People first.