Email and text messages are cheap and convenient ways to contact lots of people, which is why criminals use them.

The messages that criminals send are known as 'phishing'.

Criminals impersonate real companies like banks, energy companies and government agencies to make their phishing messages appear legitimate.

Because they are sending the same message to a lot of people at once, they can't personalise each one, but they do like to create panic, and sometimes joy.

Sometimes criminals get so excited about stealing money with their crime, they forget how to spell correctly.

But they all want the same thing - to make you click on a link or an attachment and hopefully take something from you, normally your money.

These links go to fake websites which are designed to steal your personal information, or they'll have attachments which contain malicious software.

Just remember, NAB would never ask you to provide your personal or banking details via email or text.

So just remember, don't click that link.

We're on your side.

Report phishing by forwarding the message to hoax@nab.com.au.

However, if you've provided your personal or NAB banking details to a phishing message, call NAB immediately on: 13 22 65.

For more information to help you stay safe online, visit: nab.com.au/security.