Information sheet: *Social engineering*

What is social engineering?

"Social engineering" describes any situation in which a person contacts you and impersonates someone else in an attempt to trick you into disclosing personal information or access credentials. They may contact you by telephone, email, SMS or any other means. They may pretend to be a representative of Ability WA or another business, or a government official.

Why is there a risk of social engineering following a data breach?

A cybercriminal may obtain your contact details and some personal information about you from a data breach, but not enough to access your accounts or impersonate you. Therefore, they may contact you in order to try to get additional personal information from you. They may use the information they already do know about you – from the data breach, from previous data breaches, or just from public sources – to convince you that they are genuine.

How do I protect myself from social engineering?

1. The main protection against social engineering is simply to be aware that it exists, and to be wary of any unsolicited contact that purport to be from Ability WA or a government authority or business, especially if they start asking for personal information or access credentials.
2. If you are in any doubt about whether a telephone call is genuine, hang up and contact the business or authority back on their public number. Contacting a business or authority by telephone on their public number is also the best way to check whether an email or SMS is genuine.
3. Don't trust a call or SMS just because the sender's number looks genuine, and don't trust an email just because the sender's email address looks genuine. Telephone numbers and email addresses are easily faked.
4. Be suspicious of anyone who asks you to fill in a form, log in to a page with your username and password, tells you they have detected a problem with your computer, or advises of a change in bank account details for a payment. These are common scams.
5. You can also get advice and support by contacting IDCARE, Australia's national identity & cyber support service on 1800 595 160 or at www.idcare.org. IDCARE has fact sheets about scams on its website.