Stay Safe Online with DiCureCitizen

Here is a standard guide that is issued to users when they have experienced a potential scam through their SMS or email. This booklet has provided the type of scams and how to evade them.

Here is a list of Potential Scams with some examples that will help you understand better.

1. Fake Texts or Emails

   Scammers send messages that look like they are from your bank, the government or from a delivery service

   Example:
   "Your account is currently locked due to suspicious activity. Click on the link below to fix it now"

2. Investment Scams

   Scammers send you emails and SMS texts about potential investment opportunities related to crypto, stock and real estate.

   Example:
   "Invest $5,000 today and get a 25% return in year one of investment. Got you excited? Click on this link to join now.

3. Employment Scams

   Scammers send SMS texts about potential employment opportunities usually offering outrageous pays and rates.

   Example:
   "We are currently looking for a data entry operator. The base pay is $75/hour. Want to be a part of our team? Click on this link and answer the questions.

Here are some simple safety tips Simple Safety Tips

1. STOP. CHECK. REJECT

   Stop: Take a moment and think if you are actually expecting a message like the one you received.

   Check: Check on DiCureCitizen to check if it might be a scam

   Reject: If the probability is high, delete the message and/or report it as a spam.

2. Never share your Passwords or PINs

3. Always make sure to use strong passwords and PINs

4. Do not provide your phone number and email to random websites that you visit.

5. Share your issues and concerns with your family and friends for moral support.

What should you do if you are scammed?

1. Contact the authority (for example: contact the bank in case your financial information is exposed) immediately

2. Report to Scamwatch on scamwatch.gov.au

3. Make sure to stop contact with the scammer.

Need help? Contact IDCARE Australia on 1800 595 160