REFERENCE SHEET

PHISHING

What is phishing?

Phishing is a strategy used by fraudsters that involves sending out mass emails or text messages that appear to come from a legitimate company.

These emails or text messages are used by ill-intentioned individuals to steal personal information or install malware on the recipient's computer, by encouraging them to click on links or open attached files.

Adopt this simple measure

Before you click, **verify the information** by:

1. checking whether or not the email or text message was expected
2. being aware of the types of situations that might prompt you to react:

Urgency

The goal is to create a sense of urgency to make you act quickly on a reflex.

Profit

The goal is to make you believe that you've won something even though you haven't entered a contest. Fraudsters use greed to trick you into disclosing your personal information.

Problem

The goal is to inform you of a problem with your account so that you disclose personal information in order to resolve the problem.

3. Check that the sender's email address is one you know and seems legitimate (especially the portion after the at sign [@]: Is it a company address or personal?)

4. Hover your mouse over the hyperlink (without clicking on it) to see if the link address looks legitimate and matches that of the sender's company (watch out for addresses that are almost the same).

5. Evaluate the relevance and plausibility of the email. Be suspicious and ask yourself questions! (E.g. Did you really enter a contest? Are you expecting a package? Is this the standard procedure? Is it too good to be true? etc.)

6. Never disclose any confidential information via email that could be used to authenticate your identify (e.g. SIN, credit card, birth date, password).

7. Try not to be curious or distracted by popular brands or logos which can easily be copied and look like an authentic email or website.