SMS Spoofing

Do you get an SMS that says you're being fined for a traffic violation, or that your package is unsuccessfully delivered?

Did these messages have suspicious links in them asking you to click? Beware, this could be SMS spoofing. SMS spoofing is when fraudsters send messages that may look like they come from companies like your bank, telco or even the government. It usually has a link that attempts to get your card details and OTP. Keep yourself protected and be vigilant of these types of messages.

Watch out for these red flags:

- The SMS message has a sense of urgency or has a too-good-to-be-true offer.
- Has a suspicious link leading you to a fake website.
- The fake website asks you to input your card details and your OTP.

Here are some examples:

Dear Customers, act now! Your 3022 points will expire soon. Redeem premium rewards at points center: https://rewards.life/mypoints

Click now and get the free gift!

We're reminding you that your current postpaid account's (3,022 points) is expiring today. Please redeem the prize as soon as possible:

https://bit.ly/3w4jXit?egL=dLZ0rCefh

PHLPost: Your package has arrived at the warehouse but cannot be delivered due to incomplete address details. Please confirm your address at the link.

https://phlpostd-bg.top/i (reply 1 to activate the link or copy the link to your Safari browser and open it)

REMEMBER:

- Do not click any suspicious links – it could be a SCAM.
- Always READ the SMS OTP message thoroughly and validate your online transaction. Check the AMOUNT and purpose before using your OTP.