Do not fall victim to impersonation scam calls

What is an impersonation scam call?

An impersonation scam focuses on tricking users into believe something is true through seemingly legitimate interactive automated voice messages. Victims receive calls/interactive voice messages from fraudsters impersonating representatives or officers from courier companies, banks, customs officers, the police, or government bodies.

Popular types of phone scam

Macau scam

The scammer disguises himself or herself as a representative of a government body or legitimate institution. The person then claims that the victim has outstanding loan payments or unpaid fines. The victim will later be asked to transfer funds to avoid penalties or lawsuits.

Parcel scam

The scammer claims to be calling from a courier company or the customs office, informing the victim that he or she has unclaimed packages or parcels that are being held back because they contains illegal items. The victim is then requested to transfer funds to release the parcel and avoid detention by the authorities.

e-Commerce scam

The scammer entices the buyer to purchase products with fantastic deals and later asks for further payments for things like a delivery fee, insurance cost coverage or customs taxes to claim the product. Once the payments are made, the scammer will become uncontactable.

Phishing call

The scammer tricks the victim into entering a phishing website resembling their online banking website and then invites them to change their password or transfer money. Your banking credentials will be stolen once you log in to the phishing site.

Some common signs of scam call

- Suspicious phone number.
- Delayed greeting or the use of automated voice response.
- The call comes from companies or government bodies with whom you do not have an association.
- You are invited to identify yourself by revealing personal or banking information.
- The caller tries to make you panic or rush you into decisions.
- The caller offers promotions or gifts that sound too good to be true.

What you should do if you receive a scam call

When in doubt, just hang up!

Do not share your internet banking credentials (organisation ID, user ID, passwords and OTPs) to anyone or display the information in a manner that is visible to others.

Please be reminded that the Bank or government officials will not make unsolicited requests for your sensitive information through email or by phone.

If you have accidentally disclosed any personal or banking information to a suspicious caller or if you notice any unusual or unauthorised transactions, please call us immediately at **603-8317 5200.**