We think that it will never happen to us — but fraudsters play on the fact that we might not be paying attention.

They can steal information when you are at an ATM or when you are online. Fraudsters can even impersonate your bank, the police or someone you know in order to get you to share your personal details or hand over money. They may contact you via email, SMS or phone or use malware to access your information.

At Standard Chartered, we’re committed to helping you to fight fraud so that fraudsters can’t take what is yours.

### Social Engineering

The use of phishing, vishing and smishing to access or get your personal information.

- **Phishing**: Emails with links containing malware that can access your personal information
- **Vishing**: Calls impersonating banks or companies to obtain account details
- **Smishing**: Text messages from unknown numbers containing suspicious links

### Stay protected with these tips:

- Take note of email addresses. Look out for changes such as johndoe@wahoo.com instead of johndoe@yahoo.com
- Transact on safe websites with the lock icon or ‘secure and verified’ badge at the bottom of the page
- Never reveal personal or banking information to anyone over the phone or email
- Don’t click or download software from unknown links. They may contain malware which can access personal information from your computer or phone
SIM Porting/Swapping

Fraudsters may obtain a duplicate SIM from phone companies by impersonating you. This allows them to receive OTPs and notifications from your bank.

Stay protected with these tips:

- Be alert to any notifications sent by your phone company on any unauthorised SIM change. Call them immediately if you receive one.
- Take note of long periods of network outage on your mobile; this could be an indication of SIM deactivation.

ATM Fraud

Your ATM card information can be stolen while you are at the ATM.

Stay protected with these tips:

- Be wary of people around you at the ATM.
- Ensure the machine has not been tampered with.
- Cover the keypad when keying in your PIN.
- Shred and discard your receipts.

Card Fraud

The use of cards for unauthorised or unlawful transactions.

Stay protected with these tips:

- Never share your card details with anyone.
- Keep your card in sight when making payments over a counter and ensure the correct card is returned to you.
- Check your card statements for unknown transactions.
- Shred and discard card statements, receipts, and old and expired cards.
Elder Fraud

Fraudsters target everyone, even the elderly.

Stay protected with these tips:

- Ignore calls or emails asking for personal details or payment
- Always verify the identity of the person you are dealing with
- Don’t download any attachment from unknown sources as it may contain malware
- Don’t share personal information, PIN or password

Money Mule

A money mule is someone who accepts and transfers money in return for a fee. Fraudsters recruit money mules in a number of ways.

Stay protected with these tips:

- Beware of people offering fees to receive and transfer money using your bank account
- Don’t open a bank account in your name to receive and transfer money for someone else

Fraud can be hard to spot at times, but together we can reduce the risk by following these simple steps.

SPOT THE WARNING SIGNS
Be vigilant at all times. When in doubt, verify the source of the calls, emails and/or text messages.

STOP SUSPICIOUS ACTIVITY
Do not respond to requests for personal details from unknown sources.

REPORT THE INCIDENT
If you suspect any fraudulent activity, report the incident to us immediately. The quicker the fraud is reported, the higher the chances of recovery.

Click here to view the brochure in Bahasa Melayu
Click here to view the brochure in Chinese

#DoYouSeeWhatWeSee