Sometimes it’s too late to spot a scam.

Dear Valued Customer,

We all think we’ll never fall prey to scams, but they can happen to anyone. Fraudsters will try to obtain your personal information via email, phone or SMS. This is known as social engineering.

At Standard Chartered, your security is our priority. Stay one step ahead of fraudsters with these tips.

Understand the different types of scams

Phishing

Email Fraud

Emails containing links that request for or access your personal information when clicked.

Vishing

Telephone Fraud

Calls pretending to be from banks, phone or delivery companies asking for personal information.

Smishing

SMS Fraud

SMS texts from unknown numbers containing suspicious links.

Stay vigilant and look out for these warning signs

Standard Chartered will never ask for your **PIN or password**. Such requests are likely to be from fraudsters.

Beware of **incorrect email addresses**. Look out for minor changes, such as johndoe@wahoo.com instead of johndoe@yahoo.com.

Do not click on links from **unknown emails** or websites. They may contain malware designed to spy on your online activities or steal your information.

Always verify a website's URL before you make an online transaction. Look out for the lock icon or **'secure and verified'** badge at the bottom of the page.

Watch out for SMS texts from **unknown numbers** — they may contain suspicious links or requests for personal information.

Fraudsters often lure victims with attractive prizes or rewards.
Don’t take the bait.

SPOT

THE WARNING SIGNS

Are you dealing with an impersonator?

STOP

SUSPICIOUS ACTIVITY

Never share your PIN and password.

REPORT

THE INCIDENT

The sooner you report it to us, the better the chances of stopping the fraud.

For more fraud prevention tips, visit.

To report a fraud, please call
263 242 254281-3