PROTECT AGAINST COMMON FRAUD TACTICS

Fraud can start from a seemingly harmless phone call, email, text message and even a mailed brochure. Below are four common fraud tactics that you should be aware of to protect yourself and our customers. Review the facts before providing any personal information, or making any fund transfers. Vigilance is your best protection.

ONLINE SCAMS

How it usually works: There are many online scam tactics, most of them **stem from phishing links for an online offer or a survey, with a promise of a reward** for your response. Phishing could also occur via an unsolicited email informing you to re-authenticate your password. Often, such emails impersonate well-known online companies e.g. PayPal or Amazon. Once you click on the link and/or provide your details, your hardware (computer/mobile phone) could be infected by malware and your account would be compromised.

Another popular fraud target is when you put an item for sale online (e.g. eBay, Craigslist). The buyer **will 'mistakenly' overpay for the item** and asks to return the excess payment. Unbeknown to you, proceeds from illegal gains have been masked as the excess payment and you are being used to launder money. Always be wary of anyone who purportedly pays you in excess of the listed prices.

What you could do: Check the spelling of the company in the URL. For example, Standard Chartered URLs are spelt sc.com, not standardchartered.com. When in doubt, refrain from clicking on any unfamiliar links, emails or online advertisements, and/or verify the authenticity by searching for the company's details. Similarly, before making any online purchases, check the legitimacy of the sender. For more tips on online security, visit our 'Security and You' page.

ADVANCE FEE SCAMS

How it usually works: This scam involves an upfront payment in exchange for a larger sum of money or reward. An example of this is a call informing potential victims that they have **won the lottery**. To receive the winnings**, a processing fee and/or taxes must first be paid**, usually to an offshore account. However, after the payment is made, the prize remains elusive.

What you could do: Always check the authenticity of the company/organisation offering the prize. It is important to note that Advance-Fee scams can happen through a variety of links/websites including those for employment, dating, and even charity. If in doubt, it is best to avoid entertaining such calls or responding to such communications

FICTITIOUS EMERGENCY

How it usually works: This scam usually targets the elderly and appeal to their emotional vulnerability by presenting **a dire situation of a person in need**. Often, the fraudster will impersonate the police or hospital staff/'good Samaritan' to convince the victim that his/her relative has been arrested or hospitalised and require urgent funds for bail or medical treatment.

What you could do: Do not panic. Ask for the caller's name and work/personal identity number. Usually, the caller will hang-up when probed. If you are able to obtain their work identification, authenticate the claim by contacting the said police station or the hospital, or even calling the relative in question.

INVESTMENT SCAM

How it usually works: Also known as **'Boiler Room Scams'**, an imposter impersonating a sales representative will employ hard-sell tactics to pressure you into taking up a **potentially high-returns investment offered for a very limited period**, and funds must be quickly transferred to an offshore account. Fraudsters have known to offer fake Standard Chartered Bonds in this manner, asking payments to be made to an account in Hong Kong.

What you could do: Validate the authenticity of the offer by checking the registration of the individual selling you the shares, or contacting the company whose shares are being offered. If you have any doubt, contact the bank's fraud team *before* making any payments. For more helpful tips on protection against investment fraud, visit the US Securities and Exchange Commission or the UK Financial Fraud Action websites.

If you suspect that you may have fallen prey to fraud and your Standard Chartered account has been compromised, contact your local Standard Chartered office immediately. Click here to locate your nearest Standard Chartered office.