Fight Against Fraud

Fraud can start from a seemingly harmless phone call, email, text message and even a mailed brochure. Here are some commons fraud tactics that you should be aware of. It is prudent to stay vigilant and review the facts before providing your personal information, withdrawing your funds for payments, or making any online fund transfers.

Money Mules

How it usually works: In most cases, the individual may not be aware that they are being used to transfer funds. The fraud could start from an unsolicited email informing you of the need to authenticate your password or inviting you to register your personal details to activate a limited time offer. Often, such emails impersonate well-known online companies e.g. PayPal or Amazon. Once you click on the link and/or provide your details, the fraudsters will attempt to hack into your account and use it to transfer funds.

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, the excess payment is proceeds from illegal gains and you are being used to launder the money. Always be wary of anyone who purportedly pays you in excess of your 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, avoid clicking on any unfamiliar links, emails or online advertisements, and verify by searching for the company's details. Similarly, before making any online purchases, verify the legitimacy of the sender. For more tips on online security, visit our 'Security and You' page.

Prize or Lottery Winnings

How it usually works: Fraudsters bait unsuspecting victims through a call, letter or an email informing them that they have won a large sum of money. To transfer the winnings into the bank account, victims will be asked their bank account details. In addition, payment for various expenses or taxes will need to be made before the prize can be released. Not only is access gained to the bank accounts, funds are stolen, and the non-existent prize remains illusive.

What you could do: Avoid engaging with such callers or responding to such communications. It is best to hang up immediately, or delete the emails without opening them.

Emergency help

How it usually works: This scam target the elderly and appeal to their emotional vulnerability by outlining a dire situation of a person in need. Usually, the fraudster will impersonate the police or hospital staff to inform the victim that his/her relative has been arrested or hospitalised and require urgent funds for bail or surgery.

What you could do: Do not panic. Ask for the caller's name and police/hospital 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 fraud

How it usually works: An imposter impersonating a sales representative will employ hard sell tactics to pressure you into taking up a 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 us immediately.