
# Don’t be a victim of cyber crime!

More than 100 million phishing emails are sent by fraudsters every day[1]. Stay alert and learn how to protect yourself and your loved ones from cyber crime.

## What is phishing?

Phishing is a cyber crime where fraudsters try to obtain your personal information by email, messaging apps, SMS (also known as smishing) or phone (also known as vishing). This information can be used for identity theft, payment scams and credit card fraud as well as many other forms of cybercrime. Malicious links or attachments are often included in phishing and vishing messages, designed to steal your information or infect your system with malware (malicious software).

PUBLIC

## Bank safely with us

Phishing and vishing messages may appear as though they originated from the Bank. They may include our logo or even mimic our electronic mailers. Look carefully at the sender's address for lookalike domains e.g. john@standardchartd.com.

Fraudsters can send you fake bank account statements, overdraft notices or loan cancellations. Never respond to unsolicited emails, messages or phone calls. To access our banking services, visit our official website at https://www.sc.com/.

For mobile banking, update your SC Mobile app and phone's OS regularly to ensure your security is always up to date.

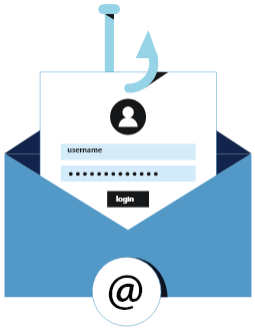
If you need to change your password, use our [i-banking website]. Never click on hyperlinks or download attachments in unsolicited emails or texts. Our official domains include sc.com


Standard Chartered will never ask you for your access code, one-time password (OTP) or credit card number. This is private information and you should never reveal these details to anyone.

Beware of unexpected prizes in fake Standard Chartered lucky draws. Fraudsters may demand a token sum from you or insist you reveal your personal information in order to win. When in doubt, always call our official hotline to verify the requestor's authenticity.

**We are happy to help you**

PUBLIC




If you receive a suspicious email allegedly from Standard Chartered, send us the email and report the incident to be.secure@sc.com. Please reach out to our customer service hotline at 02-724-1553 immediately if you suspect any unauthorised access or transactions have been made to your account. We will take steps to protect your account wherever possible. You may be required to make a police or law enforcement report.

## Together, we can STOP cyber crime.

**For more information on phishing and vishing, please visit https://www.sc.com/global/security-tips/**

Here for good

Please do not reply to this e-mail.

You are advised not to send any confidential and/or important information to the Bank via e-mail, as the Bank makes no representations or warranties as to the security or accuracy of any information transmitted. The Bank shall not be responsible for any loss or damage suffered by you arising from your decision to use e-mail to communicate with the Bank. It is essential that prior to taking into consideration any information on this site, or responding to or sending any information or materials to us in response to this mailer, you have read and understood this Important Legal Notice.