Stay safe when you bank online

Follow these tips for a
safer banking experience

sc.com/xxx

Here for good

Banking with peace of mind

Transferring funds or paying your bills is easy, using online and mobile banking.

But it is important to keep your bank account secure from any unauthorised access. Here's how you can protect your account:

Update your apps and remember to log out

Start by **regularly updating the apps and anti-virus software** on your mobile phone, tablets and laptops

Download the SC Mobile App from **Google Play or the App Store** — never from third-party sites

When making a transaction, remember to **double check the details** before you press the submit button

Always log out of the SC Mobile App or online banking session after use and never leave it running in the background

Always ensure your password is secure

When logging in to Online or Mobile Banking, safeguard your login details by **keeping them away from prying eyes**

Don't store your username, password or account number on your mobile phone

Ensure your **bank account password is unique** from your other passwords

Never share your banking login details or One-time Passwords (OTPs) with anyone
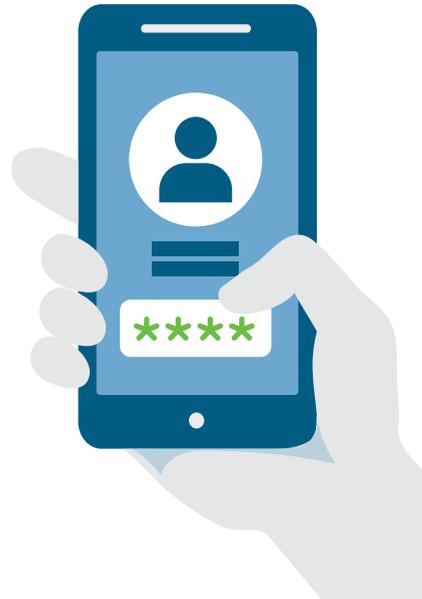
Be aware and never share

Be careful about sharing personal information like your full name, date of birth, address, mobile or phone number. These details could be used to steal your identity

Never respond to unsolicited emails, phone calls or texts. Scammers are clever at impersonating someone you trust, such as a police officer or a Bank representative

Beware of payment or fund transfer requests from people you don't know. If you are unsure, speak to someone you trust or contact us before making any payment or cash transfer

Watch out for unauthorised cash deposits or withdrawals on your account, they could be fraudulent transactions

If you receive a suspicious email, text or phone call allegedly from the Bank, please **check the identity** of the sender or caller with us immediately

Looks suspicious?
Make sure you call us!

If you notice any unauthorised access to your account or unauthorised transactions on your account close the mobile app or web browser and contact us immediately at [NUMBER].

Remember, Standard Chartered will never request for your password or security information by phone call, email or SMS.

Visit us at [URL] to learn more about our online and mobile banking services. For more information on the SC Mobile App, please visit [URL].