Identity. Information. Money.

There's more on the line than just a call.

Know the difference between a genuine call and vishing. Protect your financial information from being misused.

Knowing about vishing is the first step to protect yourself from it. Vishing is a type of fraud where a person poses as a genuine caller, may be as a bank official or an authority figure, and lures you into sharing your confidential information, that is then used for identity theft.

Here are a few pointers that will tell you how to protect yourself from vishing:

- Do not provide confidential information over the phone. The Bank will never ask for private information like:
  - One Time Password (e.g. Credit Card CVC number, Card PIN number, Internet Banking password)
  - Card/Account Information (e.g. account numbers)
  - Above information via text (SMS) messages.
- Be cautious of phone numbers, even if the number displayed is that of your bank ,as these can be spoofed to make the call appear as genuine.
- When you receive a call, ask questions and get as many details as possible.
- When in doubt, inform the caller that you will call back on the number. HSBC contact details are available here. This will help you validate the genuineness of the call.
- Do not respond to any suspicious looking e-mail, automated calls or text messages from the bank, you may wish to check with us.
- Do not share your personal information on any social sites or media (e.g. Facebook, Instagram, Twitter). Be discreet when you tweet.
- Ensure you update your contact details with the Bank to get timely alerts.

For more information on online security and good banking practices from HSBC, visit the online security website for more tips

HSBC

Together we thrive

Issued by The Hongkong and Shanghai Banking Corporation Limited in May 2018.