Protecting you always

Some criminals are using the current coronavirus outbreak as an opportunity to scam the public. This could be disguised in several forms including offers, guidance, safe haven for your money, request for donations, and contribution to relief funds amongst others. We recommend you exercise the following precautions:

- Do not click on links or attachments in suspicious emails.
- Pay particular care to some emails with titles such as “We need your support”, “Would you consider donating?”, “COVID-19 Urgent Support”, “Safety measures virus” etc.; these may not be genuine.
- Do not respond to special offers or promotions offers for Coronavirus-linked products or services without prior verification of authenticity
- Exercise caution when providing your personal or financial details on unknown websites. Do not provide any of these details by email.
- Assess the legitimacy of the sites you visit.

Remember we will never ask you to:

- disclose confidential information such as your account numbers, logins and passwords, Pin code by phone, SMS , email , Viber, WhatsApp, Facebook or any other social media and instant messaging platforms ;
- move your money to a ‘safe’ account;
- access Personal Internet Banking through a link. As a good practice, you should access our website directly to start an Internet Banking session. Change your passwords immediately if you think your personal data has been compromised.

Learn more about how you can protect yourself

HSBC