



## **Covid-19: Protect your money**

Dear customer,

In this challenging period we recognize that using our digital channels is now absolutely necessary for you and we want to reassure you that safety of your online transactions is for us a priority.

Unfortunately, some criminals are using the Coronavirus outbreak as an opportunity to scam the public. This includes offering medical products, guidance or a safe haven for money.

To this end, we would like to keep you updated on the most common fraud techniques criminals use and give you some basic tips on how to protect yourself online.

### **What online fraudsters try to achieve?**

- infect your computer or mobile and tablet device with malware and steal your identity
- send you spam and scam emails
- trick you into visiting fake websites and handing over personal information
- hack into your wireless network and intercept your data, such as passwords and usernames
- take over your computer and use it to attack other people's computers

### **What techniques do criminals use most often?**

Criminals use phishing emails, make fraudulent calls (vishing) or send out text messages (smishing) to hand over your personal information or to make you follow a link to a website which seems legitimate.

### **Tips to protect yourself online HSBC will never:**

- request by any means your User IDs and passwords
- send someone to your home to collect cash, bank cards or anything else

### **Please avoid:**

- responding to an email requesting to provide your personal details. Delete any such an email immediately
- following any links received by e-mail or posted in social media, other companies' websites, search engines etc.
- paying your business partners to a new Bank account provided to you by email. Always cross-check the payment details with your partners first
- trusting non-legitimate HSBC channels and cross-check any offers for loans, cards etc.

**Make sure that:**

- your passwords are not easy to guess and keep them to yourself
- you always have your browsers updated by using the latest versions, which meet advanced security standards
- your internet browser does not automatically save User ID & Passwords for the pages you visit.

**How to report an online fraud attempt?**

In case you suspect a scam or fraud attempt, please call 210-6962190, 24 hours a day, weekdays and holidays, or send an email to [phonebanking.requests-gr@hsbc.com](mailto:phonebanking.requests-gr@hsbc.com)

Yours sincerely,

Stelios Pirpinias

Head of Wealth Management & Personal Banking (WPB)  
HSBC Continental Europe, Greece