



Some Tips and Guidelines for secure transactions

- The Bank will not request by any mean (phone, email, etc) your User IDs and passwords, that you use to enter Bank's platforms and applications. Do not respond to calls or emails that ask for your full PIN number or any online banking passwords.
- The Bank will never send someone to your home to collect cash, bank cards or anything else.
- Always have your browsers updated by using the latest versions, which meet advanced security standards.
- Change your browsers' settings, in order not to store/ prefill user names and passwords for sites, online merchant and banking websites.
- Do not respond to emails that you are requested to provide your personal details. Do not take any action like open attached files and Delete them at once.
- Trust correspondences that come only from the Bank's official channels and take special care to random offers for loans, cards etc, which fraudulently appear to come from the Bank. In case you receive any offer, that is too good to be true, please call the Bank to validate its authenticity.
- Do not trust links that appear to redirect you to the Bank's web page. Always write the Bank's web address by yourselves and never follow any hyper link that you may receive by e-mail or find it published in social media, web pages of other companies, internet search engines, etc.
- Always perform a call back to your associates when you receive an email with new Bank account details that they prompt you to transfer money for the payment of an invoice, etc
- In case your mobile device does not operate as usual, contact immediately your Mobile Provider. It is usual not to have signal due to technical issues or limited geographical bandwidth. However, if you face unexpected and with no obvious reason signal issues, you sould confirm with your Provider that your SIM card is not deactivated.
- Do not reveal your mobile number in social media platforms.
- Register in your Bank's secure sms and email alert services, where applicable.
- Do not respond to unknown sms and calls that request you to provide account details and your registered mobile number.
- Often check the transactions in your accounts.
- In case you are a victim of any fraud type like SIM Swap, Phishing, etc or you have noted unauthorized transactions in your Bank account immediately call your Bank.