Digital Security

Avoid Storing Your Personal Information and PINs on Your Computer/Mobile Phone

Your ID certificate, Passport, Residency Card are highly important documents. Therefore, do not store scanned copy of these documents on your computer, mobile phone or tablet. Make sure you regularly follow up use and security information about the product you use. Avoid keeping your debit card PIN and internet banking PIN on your card, in your wallet or in your bag or saving it on your mobile phone.

Avoid Sharing Your Information

Interactive Banking PIN and card details, card PIN, mobile approval codes sent by SMS are your personal information. For security purposes, you must avoid sharing such information with third parties including our Bank's personnel.

Make Sure Your Computer is Secure

Make sure you use licensed operating system and programs, and regularly update your operating system and software.

Make sure you use security shields such as anti-virus, anti-spyware and personal firewall.

Avoid doing banking transactions on shared computers like in internet cafe, libraries, etc.

Avoid Replying E-mails/Calls Asking your Personal Information

Banks do not ask for your personal information or PINs via e-mails. If your passwords are asked orally, in writing or via IVR, never provide information in such cases and contact with your branch immediately.

Do not agree to take help from people who give you their phone numbers to help you.

Make Sure Your PIN's Security Level is High

Do not choose your PIN which includes such as special days and dates, phone numbers, birthday which are easy to figure out.

Enter by Writing www.isbank.iq Address Bar

To use our website, simply enter www.isbank.iq on address bar of your browser, instead of clicking on any link. Our Internet Branch uses "https" protocol .

Avoid Using Wireless Networks Whose Security is Unknown

Wireless methods such as Wi-Fi, Bluetooth, Infrared may lead to the risk of unauthorized access to mobile phones. Therefore, avoid using wireless networks whose security is unknown to you.

Avoid accepting files transferred through Bluetooth, the source and security of which is unknown to you; keep such applications off when you do not need.

Protect Your Mobile Phone via applications such as Security Code, Key Lock as well as Current Anti-Virus Software.

Malicious software can steal information on your cell phone, search something without user's knowledge or send SMS. For protection from such software;

Download mobile apps from secure app stores

Do not open e-mails and attachments received from persons you do not know

Support protection by using anti-virus software

Make Sure you Contact our Bank if your Card is Stolen or Lost

If your card is stolen, lost or stuck in an ATM, with your phone or another secure phone, call your Branch at +964 66 289 5151 or +964 771 738 7372 when you are still at ATM, and request to deactivate your card. Do not use mobiles of people you do not know.