SECURITY GUIDELINES

INVESTBANK
البنك الإستثماري

SECURITY GUIDELINES

INVESTBANK
البنك الإستثماري

At INVESTBANK, we take security and confidentiality of your information very seriously. We are committed to protect you while enjoying our state-of-the-art electronic services by continually improving and developing our security measures.

Here we outline a few steps you should take to keep your personal information, accounts and transactions safe:

PASSWORD SECURITY

Your password is the access key to your online accounts (e.g. iBank), a person knowing your password can access your accounts and commit frauds. So, it is very important that you secure your password.

The following tips will assist you in protecting your password:

- DO NOT share your password with others.
- DO NOT use the same password for multiple accounts. For example, password of your iBank account should be totally different than password of your personal email.
- Choose a 'good' password. A 'good' password is one that difficult for others to guess.
- Choose a password you can remember without writing it down.
- Change your password regularly.
- Take care when entering your password or PIN to ensure that nobody is watching.

How to create a 'good' password?

- Use only strong password with a combination of upper/lower case letters, numbers and special characters.
- The longer the password, the tougher it is.
- Avoid using personal information. It is very easy for someone else to guess things like your birthday, name of your secondary school and other similar details.

Using a passphrase to remember your password is a good choice. Think up of a sentence you can easily remember, and use it to create your own password. For example, taking the first letter of the following quote "Be the change you wish to see in the world" forms a strong password like "B+cUw2c".

Remember: Do NOT reveal your password or PIN to anyone, INVESTBANK will never ask you for this. If you are asked for such information over phone, email or any other mean, it's probably a scam.

SOCIAL ENGINEERING:

Social engineering is the practice of using human interaction to manipulate a person into providing sensitive information. Social engineering attacks attempt to exploit tendency of people to trust others in order to steal their information and commit frauds. For example, somebody can call you pretending to be from your bank and request you to provide some kind of sensitive information.

Social engineering is carried out through variety of forms such as email, telephone calls, and text messages (SMS), and uses different techniques such as spoofing and phishing.

SPOOFING

Spoofing is a techniques used to masquerade as a trustworthy entity. A 'spoofed email' is when the sender purposely alters part of the email to appear as originated from someone other than the actual source.

Website spoofing, which is other kind of spoofing, is the act of creating a fake website that looks exactly like a legitimate website published by a trusted organization.

PHISHING

Phishing is the act of deceiving customers to acquire sensitive information (e.g. credit card details, passwords, personal details) by masquerading as a trustworthy entity in an electronic communication such as emails and text messages. Usually, phishing attacks use spoofing techniques to achieve their objectives.

Example:
Customers may receive forged emails requesting them to reset their online banking password for maintenance purposes by clicking on a link inside the email. When a customer clicks on the link, the customer will be directed to a spoofed website that is made to look exactly like the legitimate website that belongs to the bank. Since the faked website is well-designed to look similar to the legitimate one, the customer will enter his/her password to complete the fake reset process.

Protection Tips:

- Do not respond to suspicious emails and text messages, or click on any links inside these emails. Please call our Call Center to inquire about any emails and messages seem to be sent from INVESTBANK.
- Whenever you receive a phone call from somebody pretending to be from INVESTBANK, you are advised to:
  * Verify that the phone number belongs to INVESTBANK.
  * Verify identity of the requestor by asking information such as the caller's name and department.
  * Verify phone number of the caller.
- Always pay attention to the web address (URL) of the websites you are visiting. It is preferred to type URL of the websites you are visiting (e.g. iBank website) into your browser by yourself rather than click on links you might see in an email, text message, or another website.
- Avoid using websites when your browser displays certificate errors or warnings. Remember that, web address of iBank always starts with https:// (the "s" is for secure) rather than http://
- Monitor your account transactions regularly to detect fraudulent activities.
- Report to us immediately via +962(6)5001515

GENERAL TIPS TO MAINTAIN SECURITY OF YOUR INFORMATION:

- Use your common sense to assess reasonableness of the request.
- Secure your PC.
- Maintain active, up-to-date antivirus.
- Keep your operating system (e.g. Windows) and internet browser updated with the latest security patches.
- Avoid accessing your iBank account from shared PCs or in public areas.
- Always 'log out' from your iBank account after finish, and close the bowser.

Tips to secure your credit cards:

- Don't share your credit card or PIN with others.
- Use your credit card and your personal information only on websites you trust.
- DO NOT let retailers take your card out of sight, whatever excuse they may give you.

For any information, please contact our call center on +962(6)5001515