إتقان
كابيتال
ITQAN CAPITAL

Important Guidelines for our clients on Information Security

Please protect yourself by considering the following:

Precautions on passwords:

- Do not disclose your account passwords to anyone.
- Change your password frequently at least every 90 days.
- Use passwords of at least 8 characters long mixing letters, numbers and special characters.

Precautions on internet browsing:

- Do not connect to un-known Wi-Fi especially when trying to access your bank or investment accounts.
- Ensure that your PC is secure by installing a known anti-virus program and keeping it up to date.
- Banks & Investment Accounts are protected through secure websites which can be seen through the "lock" indicator.
- Do not visit your bank or investment accounts through links received through e-mails. It's best to write directly the web address or access through your saved favorites.
- Delete your browsing history if the PC is a public one or not yours.

Precautions on your e-mail:

- Ensure that you have a secondary authentication method for your e-mail account like your mobile number.
- Do not open e-mail attachments from an un-known person and check the links before you click on them.
- When you receive an e-mail warning you about an attempt to access your account, it's best to change the password by going directly to that website.

Precautions on use of your personal PC:

- Make sure that you have installed an anti-virus program on your PC and that updates are done automatically and frequently. Do a full scan on your PC on frequent basis.
- Ensure that your firewall is enabled.
- Ensure that updates for the Operating system, and other browsing programs are done frequently.
- Do not install illegal programs or programs from non-trusted sources.
- Always scan any external flash or hard drives for viruses before copying to or from them.

- If your PC is portable then you should protect with a power-on password so that your information cannot be accessed when lost or stolen.

Precautions on your personal information:

- Do not disclose your personal information to anyone like your full name, ID number, corresponding address, and account numbers. You may receive calls from a phony person claiming to be your bank representative so you need to check if the source is legitimate.
- Do not disclose your bank account or credit cards details if you cannot verify the source is legitimate.

If you see any unusual activity in your account with us, please contact us by phone on +966-12-2347000 or through e-mail to customersupport@itqancapital.com

Important Topics on information security threats for our clients

- **Hacker:** a person or an entity that seeks and exploits weaknesses in a computer system or computer network. Hackers may be motivated by a multitude of reasons, such as profit, protest, challenge, enjoyment, or to evaluate those weaknesses to assist in removing them. A hacker may use the information gained for personal gains such as accessing your bank or investment accounts.

- **Phishing:** the illegal attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication. An e-mail may direct users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Another way is to lure someone to install a program that illegally allows the hackers to gain access to information.

- **Social Engineering:** a psychological manipulation of people into performing actions or divulging confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional "con" in that it is often one of many steps in a more complex fraud scheme. Common methods used to get at your information, are phone calls, searching through your garbage and direct persuasion.

- **Computer virus:** is a malware program that, when executed perform some type of harmful activity on infected hosts, such as stealing hard disk space or CPU time, accessing private information, corrupting data, displaying political or humorous messages on the user's screen, spamming their contacts, or logging their keystrokes. However, not all viruses carry a destructive payload. Users install antivirus software that can detect and eliminate known viruses when the computer attempts to download or run the executable (which may be distributed as an email attachment, or on USB flash drives, for example).

  Antivirus software must be installed to remove the threats but the software must be updated regularly so that new viruses can be dealt with. Infection can occur through direct infected external drives or indirectly through internet files downloaded from websites or social media software.