JSC Isbank Georgia Digital Security Guide

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

Your ID certificate is a highly important document. Therefore, do not store scanned copy of your ID certificate on your computer. 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, Turkish ID Number, Bankamatik and credit card details, card PIN, mobile approval code sent by SMS and one-time passwords 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, 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 call our Contact Center at **+995 322 44 22 44**.

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 or foundation year of your favorite team which are easy to figure out.

Enter by Writing www.isbank.ge Address Bar

To use our website, simply enter www.isbank.ge on address bar of your browser, instead of clicking on any link. Our Internet Branch uses "https" protocol and also "EV SSL (Green Address Bar).

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