TIPS TO PROTECT YOUR PERSONAL DATA

Dear customers,

Investbank AD applies different security mechanisms to protect your personal data and to ensure the security of your online payments using the Internet Banking Service.

However, the security of your e-mail and computer system can be attacked by various viruses and malware designed to steal personal information, such as: passwords, access codes for Internet banking, debit/credit card numbers, numbers of other personal documents, etc.

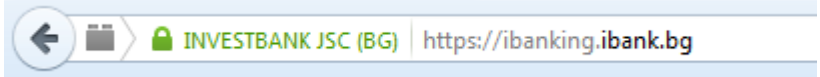
We recommend the following measures that you can take to protect yourself from potential online fraud:

- Never reveal your personal information by phone, SMS or email;
- Install antivirus software on your computer and mobile device, run regular scans and watch out for updates of its definitions;
- Use "strong" passwords;
- Pay attention to the received emails and observe the following:
  - o If the e-mail contains a link to a website, always check where it will "take" you before clicking on it. Place your cursor over the URL link and check whether the address is the same as the address which appears in the pop-up window - if they are different, do not open this link;

  - o Do not trust emails that direct you to sites where you have to fill in your username, password or other personal information;
  - o Pay attention to the text. Most fake e-mails contain text with spelling and syntax errors. These errors create the impression that the text was written by someone who is not fluent in Bulgarian. Immediately delete such e-mails!
- Recognize the protected page of the Internet Banking Service of Investbank AD:
  - o Before you enter your Username and Password, look for evidence that the website you have chosen uses an encrypted channel for data exchange. A sure sign of whether the received messages on the screen are from the Internet Banking system of Investbank AD is the presence of "green" coloring of the address field, the padlock next to it and the image with the stamp "Norton Secured". The following figures show such examples:

    - Internet Explorer

    - Mozilla Firefox



Head Office

85, Bulgaria Blvd. 1404 Sofia, BG
T +359 2 818 61 23, 818 61 24, F + 359 2 854 81 99
SWIFT IORTBGSF
www. ibank.bg
office@ibank.bg

- Google Chrome

- Stamp "Norton Secured"

- Should you have any doubts concerning non-standard or unknown message and/or circumstance when you use the Internet Banking service of Investbank AD, immediately contact the Call Center on **0700 12 555** /for subscribers of BTC it is at the price of a local call throughout the country/.

ADDITIONAL MEANS OF PROTECTION

Antivirus Protection
Viruses can damage your computer, destroy data or, in some cases, send personal information or passwords entered during the use of the system by unauthorized persons. The use of reliable and updated antivirus software will reduce the probability of such an adverse event.

Secure Password
Use secure passwords consisting of a combination of letters, numbers and other characters such as "@","!", etc. Change your password often - every 1-3 months.

Use only certified computers
Try to avoid using IB in the presence of other people or in public places (in internet cafes or computers used by people other than you). Also avoid public WiFi connections, unprotected by passwords.

Do not leave your QES on the computer
After finishing working with your Qualified Electronic Signature (QES), always remove it from the computer and never leave the device/chip-card unattended!

Pay more attention
Do not leave unattended your personal mobile phone or token to make sure that it is not used by another person without your knowledge!

Exit from the system
It is essential after you have finished using IB, to finish the session by pressing "Изход" (Exit) instead of simply close the browser window. This ensures the interruption of the secure connection that has been established by logging into your Internet portal.

COMMON ATTEMPTED FRAUDS

PHISHING

Online scam aimed at stealing user names and passwords.

The most common online phishing scam starts with an e-mail that looks like an official notice from a trusted source, such as a bank or credit card company. The message may seem legitimate and contain the logos of the organization and the email address may resemble that of the company on whose behalf the message is sent.

The e-mail recipients are directed to a fake website that invites them to provide confidential information such as name and password to access internet banking services, bank card number, CVV\CVC or other data.

DO NOT SUBMIT confidential information relating to your access to the Internet banking services or your bank card via the Internet or phone.

PHARMING

Another method using fake web sites, but without using e-mail messages.
Pharming scam is implemented through the so called "DNS poisoning" attach or by changing the "hosts" file in the victim's computer. In this way it redirects the traffic from a particular web site to another, which is its replica and aims at stealing sensitive information, such as username, password, etc. In the event of "DNS poisoning", the DNS server translates the addresses of the websites you type in the address bar of the web browser into IP addresses. For example, when you type www.ibank.bg, your computer will turn to the DNS server of your Internet provider to learn the IP address of the site and reopen it. If it is replaced with another address, when typing www.ibank.bg, the request will be redirected to a server containing a replica of the Bank's website.
The users might not know about the fraud, because they have typed themselves correctly the address of the website, not knowing that they are victims of "DNS poisoning" attack.

VISHING

Option of the phishing method using e-mails that contain a phone number.
In this case, users are advised to call to confirm their user IDs or other secret information. The e-mail may also contain a virus infecting the victim's computer and providing full access to the data, including bank certificates.

Important !!! In no way will the Bank request your confidential information, such as username and password for access to Internet Banking or bank card information, such as: card number, PIN, expiration date and CVV/CVC.
We recommend that if you have any doubts that you have become a victim of Internet fraud, immediately contact the Call Center of the Bank on **0700 12 555** /for subscribers of BTC it is at the price of a local call throughout the country/ and ask to have your user profile blocked for access to Internet banking or your bank card.