

## General tips for increasing the security of using First Investment Bank's internet banking

Dear Clients,

First Investment Bank (Fibank, the Bank) provides you with high level of protection and security when accessing the Virtual Branch; however, to provide effective security we need your help. Please, observe the following recommendations:

1. You are accessing the internet banking applications (the virtual branch) by username, password, electronic signature and/or combination of PINt (personal identification number) of the Token device, known only by its holder, and a one-time password (TAN), generated by the Token under a complex algorithm in compliance with all applicable cryptography and security standards. After you first visit to Fibank's virtual branch:

- Change your user name. (Please, refer to the section Settings/Changing the Username) The username must contain only Latin characters and digits, and must have a length between 3 and 32 symbols. Chose a username that is longer and is not in anyway revealing your first and last name.
- Chose your initial password. Use a password that is at least 7 symbols long and is a combination of lowercase letters, uppercase letters and digits. Password shorter than 7 symbols or containing only letters and digits can be easily guessed. Do not disclose your password to anyone. The password is personal.
- Change your PINt (personal identification number) of the Token device. You have to create new PINt from 4 to 8 numbers.

1.1. Do not give your username, password, electronic signature and Token device to any other persons. If members of your family or employees of your company need access, please, register another profile for them and they will receive their own usernames and passwords.

1.2. Do not write down or store your username and password on paper or on another permanent electronic or other media.

1.3. Enter your username and password only on the internet site with URL starting by: **https://efibank.bg**. If you receive a message, or if you are notified by any other way of a sudden change in the procedure for entering your login credentials and identification, please, do not take any actions and notify immediately the bank.

2. At least once a month change the PIN code of your UES and the PINt of your Token used to access e-fibank.

3. When you quit working with your electronic signature, it is obligatory to switch it off. Don't leave your electronic signature switched on in your computer, when you are not working with it. Keep it in secure place.

4. If you are changing the people the list of people authorized to access your account(s), the power of authority is cancelled or expires, please, duly notify the Bank.

5. When you finish your session n the virtual branch or you plan to leave the computer unattended, please, press Exit to terminate the open session with the bank. This will terminate your session, otherwise it will remain active for another 15 minutes.

6. Use reliable antivirus software for your computer used to access Fibank's virtual branch and keep them updated. Install and use antispymware software, anti-spam software for your email and updated persona or corporate firewall. Monitor the warning messages for viruses and especially Trojans. They can be used for

identity and personal data theft. Usually viruses and Trojans are installed automatically when you click on links, open applications in your email or download software of entrusted sources.

7. Use updated operating system and software. Preferably your antivirus software must be maintained by an IT professional. Do not use beta versions of the operating system and the software.

8. Update regularly the software on your computer. This way you can be sure that your operating system, antivirus and other scans are working optimally to protect you.

9. Avoid using the virtual branch from public computers and public hotspots with internet access (such as internet clubs, cafes, libraries, etc.) and from computers where software of sources that are not trusted is installed. We recommend to protect the access to your computer with a password, especially if it is accessible to other members of your family or roommates.

10. Regularly and carefully review the data you are receiving. Verify the sender of the email messages received by you and if you receive suspicious messages, do not open them and do not start the attachments. If something worries you, please, notify the bank on the contact telephone numbers or via email.

11. Upon receiving suspicious email message keep in mind the following:

a) Malicious email messages for fraud or information theft are usually messages with the following characteristics:

- they are requesting personal information by stating different reasons (such as technical, renewal, termination of services, etc.) Fibank does not request personal information for any reason.

- contain links, which require confirmation of personal information (the links are usually shortcuts to certain internet pages, which are loaded by clicking with the left mouse button over the link); do not use such links sent to you by email. The virtual branch does not communicate with its clients by sending links.

b) Do not open any attachments to this type of email messages.

c) First Investment Bank will never ask you to sent PINs, passwords or other confidential information via email, and will never sent emails requiring you to all call a particular phone number and disclose any personally identifiable and/or identification data. If you receive such email message, do not follow the instructions therein.

12. Do not visit sites that require you to disclose personal information concerning your access and identification to the Virtual branch or any other confidential documents.

13. Be extremely careful when you disclose financial and other information on internet sites, especially on Facebook and other social networks. Please, verify the authenticity of the site and the security of the communication protocol.

14. Always access the virtual branch by entering the following URL: <https://e-fibank.bg> in the address field of the internet browser. All information exchanged with the bank is encrypted and is transferred by using the SSL protocol, and each web page of the virtual branch is accessible only via **[https://e-fibank.bg/](https://e-fibank.bg)**

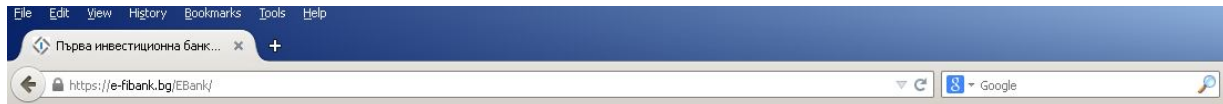
15. For maximum security use the following browsers: Internet Explorer version 6.0 or later or Mozilla Firefox version 2.0 or later.

16. The site of Fibank's Virtual Branch is identified (presented) to the clients by a server certificate issued by Thawte SGC CA ([thawte.com](http://thawte.com)). When you load the page of [e-fibank.bg](https://e-fibank.bg), an icon of a lock appears near the address field or in the lower corner of the browser depending on the type and version of the browser used.

### MS Internet Explorer

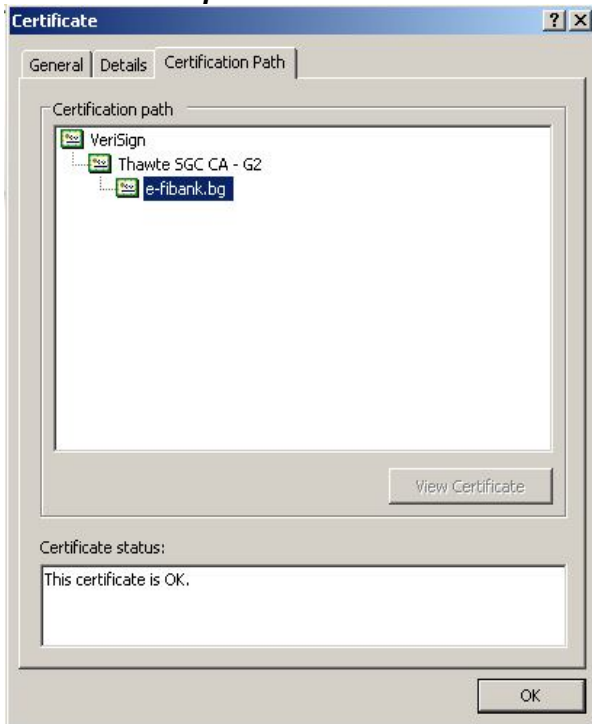


### Mozilla Firefox

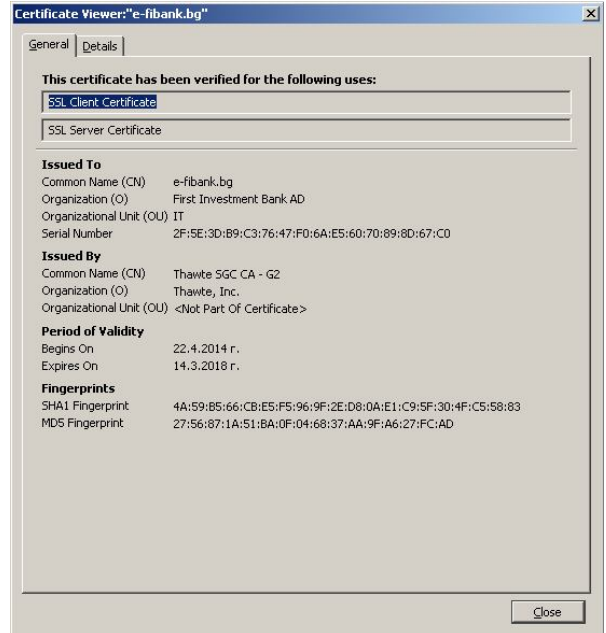
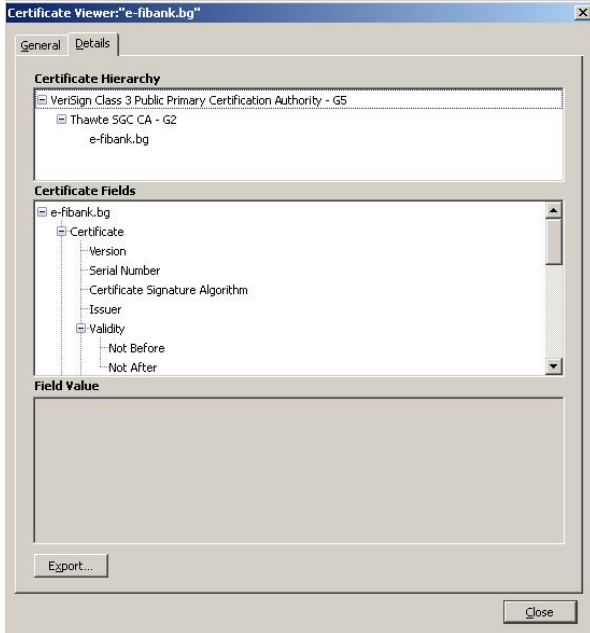


By clicking on the lock icon you will get more information about the server certificate of the page, which must be issued to e-fibank.bg.


### MS Internet Explorer



## Mozilla Firefox



In addition on the main page there is a SSL logo of thawte.com for online verification of the identity of our domain.

[ verity SGC SuperCert ]

[ valid certificate ]

Without an SGC-enabled certificate on a site, site visitors using certain older browsers and many Windows 2000 users will only receive 40- or 56-bit encryption. **thawte** is one of a very few Certificate Authorities (CAs) with SGC-enabled SSL Certificates that can provide 128- or 256-bit encryption to the most website visitors.

Authentic Sites use **thawte** SGC SuperCerts to offer secure communications by **encrypting** all data to and from the site. **thawte** has checked and verified the company registration documents, the site's registered domain name, and the authorizing contact at the company all according to the strongest identity authentication standard today.

This information is included in the SSL certificate that we issue. This enables you to check the site's validity yourself. Always **check** a site's certificate before entering any sensitive information. Below are the details for certificate: **FIRST INVESTMENT BANK AD**

[ organization ]	FIRST INVESTMENT BANK AD
[ domain ]	e-fibank.bg
[ country ]	BG
[ current status ]	<b>Valid</b>
[ valid from ]	22-Apr-2014
[ valid until ]	13-Mar-2018

[ buy ssl certificates ]

[ more information on the extended validation standard ]

[ consumer guidelines: how to know whether a site is secure ]

[ conditions of use of the **thawte** trusted site seal ]

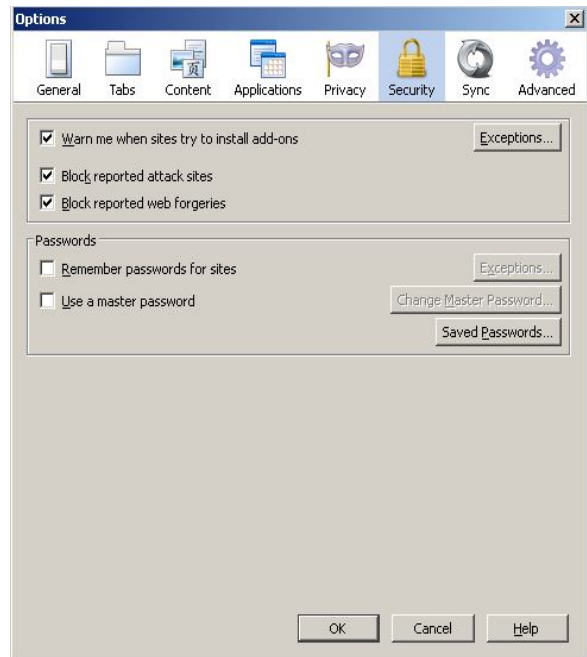
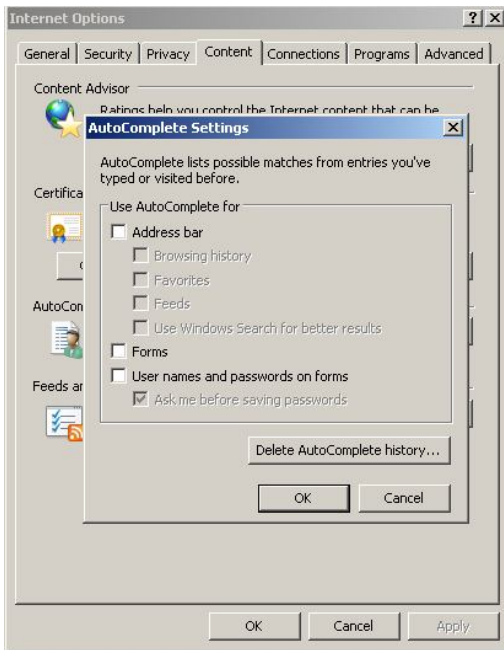
[ click here to view **thawte**'s certificate practices ]

17. Recommended settings of the web browser for using Fibank's virtual branch:

- Turn off all browser options for automatically remembering and completing web addresses, user names and passwords.
- Regularly clean the browser history (temporary files, cookies, stored user names, passwords and web forms).
- We recommend you to allow cookies only from trusted sites including e-fibank.bg and block all popup windows.

**MS Internet Explorer**

**Mozilla Firefox**



- We recommend you to allow cookies only from trusted sites including e-fibank.bg and block all popup windows.

**Example:**

In MS Internet Explorer go to the Tools menu -> Internet Options -> Privacy and chose high level of security from the slider, then add the addresses of the trusted web sites and check the option to block pop-up windows.

