Fibank
Първа инвестиционна банка

Основни препоръки за повишаване сигурността при работа с интернет банкирането на ПИБ АД

Уважаеми клиенти,
Първа инвестиционна банка (ПИБ, Банката) Ви осигурява високо ниво на защита и сигурност при достъп и използване на Виртуалния банков клон, за което се нуждаем и от Вашето съдействие. За целта е необходимо да спазвате следното:

1. Работата с приложението за интернет банкиране се осъществява чрез потребителско име, парола, електронен подпис и/или комбинация от TAH и ПИНт - чрез въвеждането на валиден ПИНт и TAH (уникален шифрован, еднократно валиден цифров код, който се генерира чрез специализирано електронно кодиращо устройство (Token), при спазване на всички стандарти за криптография и сигурност. След първоначален вход във Виртуален банков клон на ПИБ:

- Сменете Вашето потребителско име. (Виж секция 'Настройки/Промяна на потребителско име'.) Потребителското име трябва да съдържа само латински букви и цифри, и да е с дължина между 3 и 32 символа. Използвайте потребителско име с по-голяма дължина, което не е свързано с Вашето име или фамилия.

- Сменете Вашата първоначална парола. Използвайте парола с дължина поне 7 символа, представляваща задължително комбинация от малки, големи букви и цифри. Парола с дължина, по-малка от 7 символа или само от букви или цифри лесно може да бъде разкрита. Не разкривайте на никого своята парола - тя е лична.

- Сменете Вашия ПИНт за Token устройство. Използвайте парола с дължина от 4 до 8 цифри. Не разкривайте на никого своя ПИНт - той е личен.

1.1. Не преотстъпвайте потребителското си име, паролата, електронния си подпис и Token устройство на трети лица.
Ако е необходим достъп на член на семейството Ви/служител на фирмата Ви, направете отделна регистрация за него - той ще получи собствено потребителско име и парола.

1.2. Не съхранявайте на хартиен или друг траен носител, включително в електронен вид, потребителското си име и парола.

1.3. Въвеждайте своите потребителско име и парола само чрез интернет страница с адрес, започващ по следния начин: **https://e-fibank.bg**. Ако получите съобщение или по друг начин бъдете уведомени за извънредна промяна на начина за въвеждане на средствата Ви за достъп и идентификация в e-fibank, не предприемайте действия и незабавно уведомете Банката.

2. Променяйте ПИН кода на Вашия КЕП и ПИНт на Token устройствата, които използвате в e-fibank, поне веднъж месечно.

3. Когато приключите работа с Вашия електронен подпис (КЕП), задължително го изключвайте от компютъра. Не оставяйте Електронния подпис включен в компютъра, когато не работите с него. Съхранявайте го на сигурно място.

4. При промяна на упълномощените лица за достъп, изтичане срока на упълномощаване или оттегляне на пълномощни, уведомявайте Банката своевременно.

5. При преустановяване на работата с Виртуалния банков клон или оставяне на компютъра Ви без надзор използвайте "Изход" за прекъсване на сесията с Банката. Това прави Вашата сесия невалидна незабавно, вместо още 15 мин. активна.

6. Използвайте антивирусни програми на компютъра, от който ползвате Виртуален банков клон на ПИБ и следете за тяхното обновяване. Инсталирайте и използвайте анти-спайуеър софтуер, софтуер за филтриране на пощата и актуален персонален или корпоративен Firewall. Следете за предупредителни съобщения за наличие на вируси, особено от типа „Троянци" (Trojans). Те могат да се използват за кражба на лична информация. Обичайно се инталират автоматично, когато следвате линкове, отваряте приложения от e-mail или сваляте софтуер със съмнителен произход.

7. Използвайте максимално актуализирани операционна система и софтуерни продукти. Препоръчително е Вашият антивирусен софтуер да бъде поддържан от специалист. Не използвайте Бета - версии на операционната система и на софтуерните продукти.

8. Подновявайте периодично софтуера на своя компютър. По този начин ще подсигурите вашите операционни системи, контроли за сканиране на вируси и други програми с подобно превантивно предназначение да функционират възможно най-добре.

9. Избягвайте да ползвате Виртуалния клон от публични места за достъп до Интернет (интернет клубове, кафета, библиотеки и други) и от компютри с инсталиран софтуер с неясен произход. Препоръчваме да защитите достъпа до личния Ви компютър чрез парола, особено ако достъп до него имат и други членове на вашето семейство (лица, с които съжителствате).

10. Редовно и внимателно преглеждайте данните, които получавате. Проверявайте подателя на получените от Вас e-mail съобщения и при получаване на съмнителни такива, не ги отваряйте, както и не стартирайте прикачените файлове. Ако нещо ви смути, уведомете Банката на обявените телефони или със съобщение свободен формат.

11. При получаване на съмнителни e-mail съобщения имайте предвид следното:

а) E-mail съобщенията, целящи измама или кражба на данни, обикновено са общи съобщения със следните особености:

- с тях се изисква лична информация, като причините могат да са различни (технически, подновяване на валидност, прекратяване на услуги и други). ПИБ не изисква по никакъв повод подобна лична информация;

- съдържат конкретни линкове, изискващи потвърждаване на лична информация (линкът представлява препратка към дадена интернет страница (сайт), зареждането на която става с кликване на левия бутон на мишката върху линка); не използвайте посочените в подобен тип email линкове. ПИБ не комуникира чрез линкове с клиентите си;

б) Не отваряйте каквито и да било приложени файлове към подобен тип e-mail.

в) Първа инвестиционна банка АД не изисква от Вас изпращането на пинове, пароли за достъп или друга конфиденциална информация по електронна поща, както и не изпраща по електронна поща съобщения с текст, в който се изисква да се обадите на посочен телефон и да предоставите информация относно идентификационните Ви данни. В случай че получите подобни съобщения, не изпълнявайте посочените инструкции.

12. Не посещавайте сайтове, изискващи от Вас предоставянето на лична информация за средствата Ви за достъп и идентификация във Виртуалния клон или на друга конфиденциална информация.

13. Бъдете особено внимателни, когато въвеждате финансова или друга лична информация в интернет сайтове, особено в блогове и социални мрежи, като например Facebook. Проверявайте за автентичността на сайта и сигурността на комуникационния протокол.

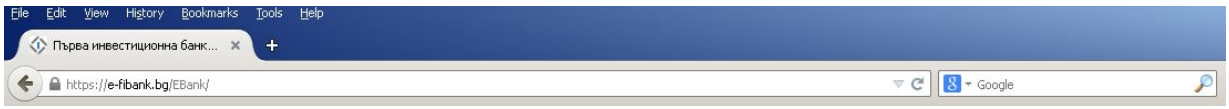
14. Отваряйте страницата на интернет банкирането, като винаги изписвате https://e-fibank.bg в зоната за посочване на интернет адреса на браузера. Цялата информация, която обменяте с нея, е криптирана и се осъществява по SSL протокол, като всяка уеб-страница в системата е достъпна само през **https://e-fibank.bg**

15. За максимална степен на сигурност използвайте браузери Internet Explorer версия 6.0 и по-късни или Mozilla Firefox версия 2.0 и по-късни.

16. Интернет страницата на ПИБ се идентифицира /представя/ пред клиентите със сървърен сертификат, издаден от Thawte SGC CA /thawte.com/. В момента, в който заредите страницата на e-fibank.bg, до интернет адреса или на най-долния ред на браузера, в зависимост от типа и версията му, се появява ***катинар***.

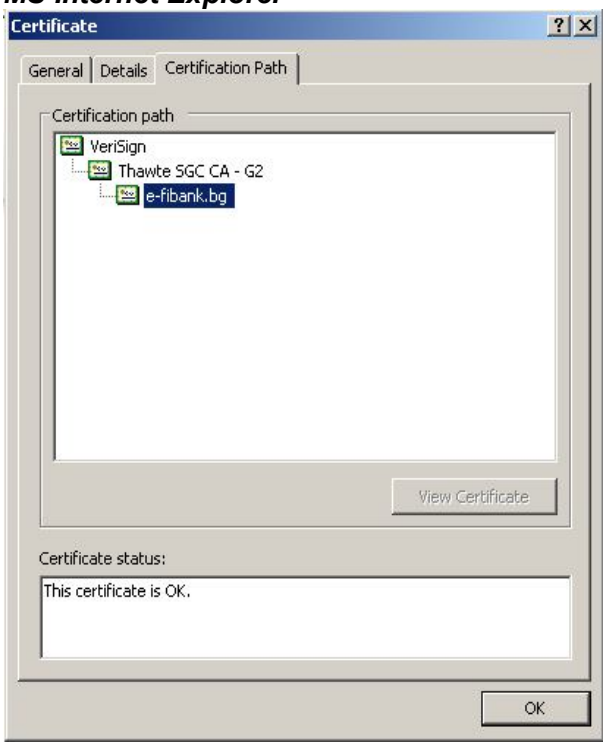
MS Internet Explorer

Mozilla Firefox

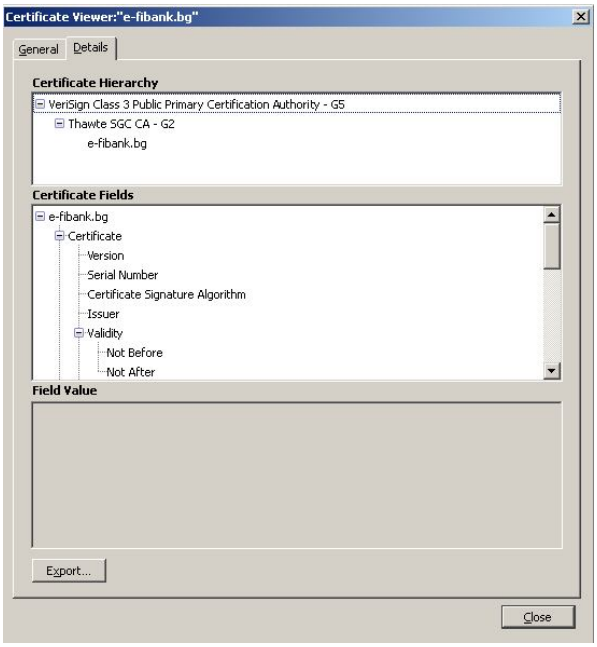


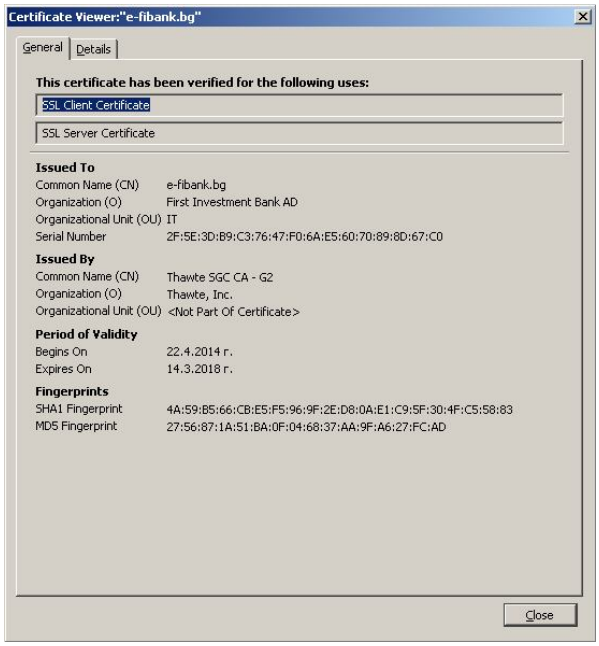
Като кликнете върху него, ще получите информация за сървърния сертификат на страницата, който задължително трябва да е издаден на /Issued to/ e-fibank.bg.

MS Internet Explorer



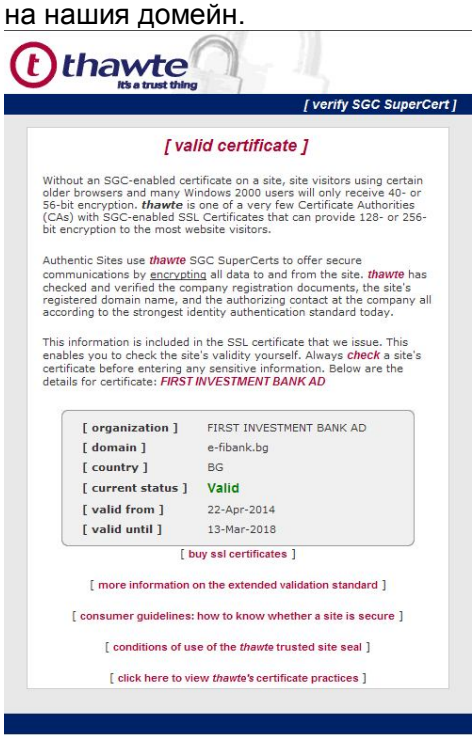
Mozilla Firefox





Допълнително на главната страница има SSL лого на thawte.com за онлайн проверка на идентичността на нашия домейн.

За SSL сертификатите



17. Препоръчителни настройки на браузера при работа с интернет банкирането на ПИБ АД:

- Изключвайте всички опции на браузера, които автоматично запомнят и дописват уеб адреси,

потребителски имена и пароли.

- Периодично изтривайте историята на браузване /временни файлове, cookies, съхранени потребителски имена, пароли и уеб форми/

MS Internet Explorer

Mozilla Firefox

- Препоръчваме Ви да разрешите cookies само на проверени от вас страници, между които и за e-fibank.bg, както и да блокирате появяването на така наречените pop-up прозорци.

Пример:
В MS Internet Explorer се влиза в меню Tools -> Internet Options -> Privacy, избира се високо ниво на сигурност и от бутона Sites се добавят адресите на разрешените страници, и се маркира блокиране на Pop-up.