Основни препоръки за повишаване сигурността при работа с електронно банкиране “Моята Fibank” и Мобилното приложение на ПИБ АД

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

1. Работата с електронното банкиране на Банката се осъществява чрез потребителско име, парола, електронен подпис или комбинация от ТАН и ПИНт - чрез въвеждането на валиден ПИНт и ТАН (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 в електронното банкиране „Моята Fibank” (Моята Fibank):

- Сменете Вашето потребителско име. (Виж секция „Настройки/Лични данни/Потребителско име“.) Потребителското име трябва да съдържа само латински букви и цифри, и да е с дължина между 6 и 24 символа. Използвайте потребителско име с по-голяма дължина, което не е свързано с Вашето име или фамилия. Сменете Вашата първоначална парола. Използвайте т.н. „силна” парола, която да съдържа комбинация от главни, малки букви и цифри и да бъде поне с 8 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. От съображения за сигурност не използвайте за парола някое от следните: име и рождена дата; поредица от числа/букви в ред (12345,abcd и други), повторение на знаци като ааа111. Сменяйте периодично Вашата парола за достъп;

- Не използвайте една и съща парола за достъп до различни акаунти за електронно банкиране, имейли и други;

- 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://my.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 Моята Fibank, не предприемайте действия и незабавно уведомете Банката.

2. Променяйте ПИН кода на Вашия КЕП и ПИНт на Token устройството, което използвате в Моята 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 в Моята Fibank 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 Моята Fibank 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 инсталират 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 Моята Fibank 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 e-mail 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 в Моята Fibank 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 Моята Fibank, като винаги изписвате https://my.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://my.fibank.bg**.

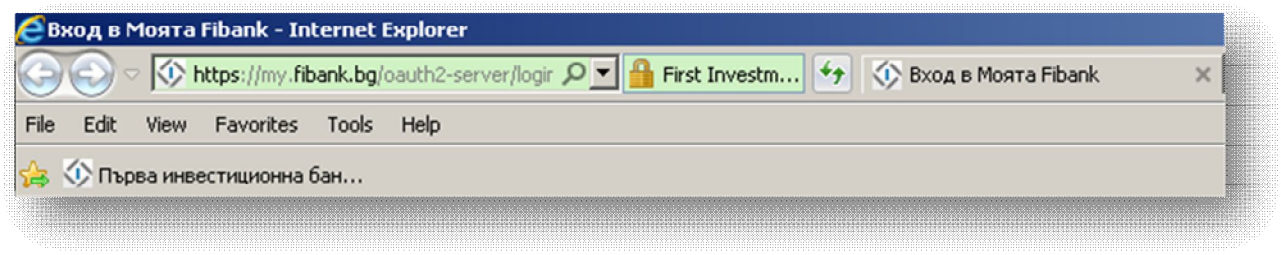
15. За максимална степен на сигурност използвайте браузери последна, официална версия на браузърите.

16. Минимални изисквания за браузърите:

    - Internet Explorer 9
    - Mozilla Firefox 16

17. 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 **https://my.fibank.bg**, до интернет адреса или на най-долния ред на браузера, в зависимост от типа и версията му, се появява ***катинар***.

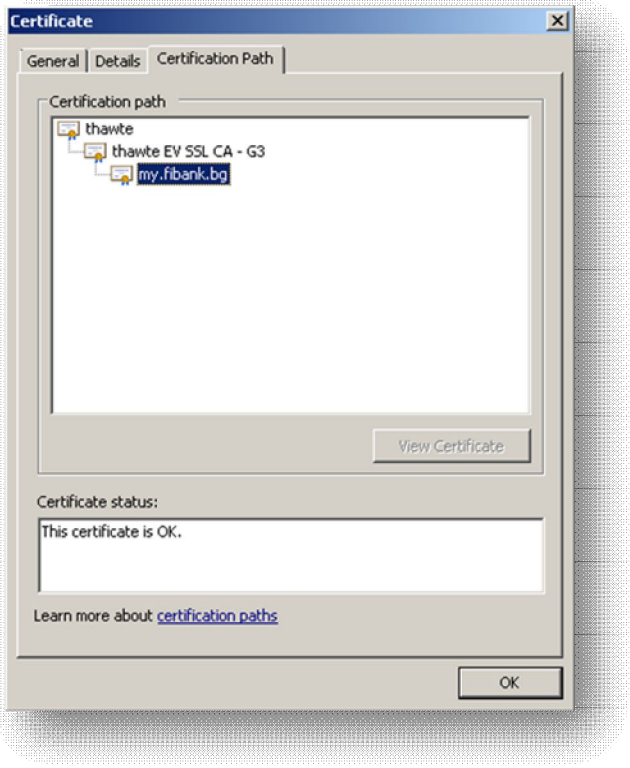
Internet Explorer

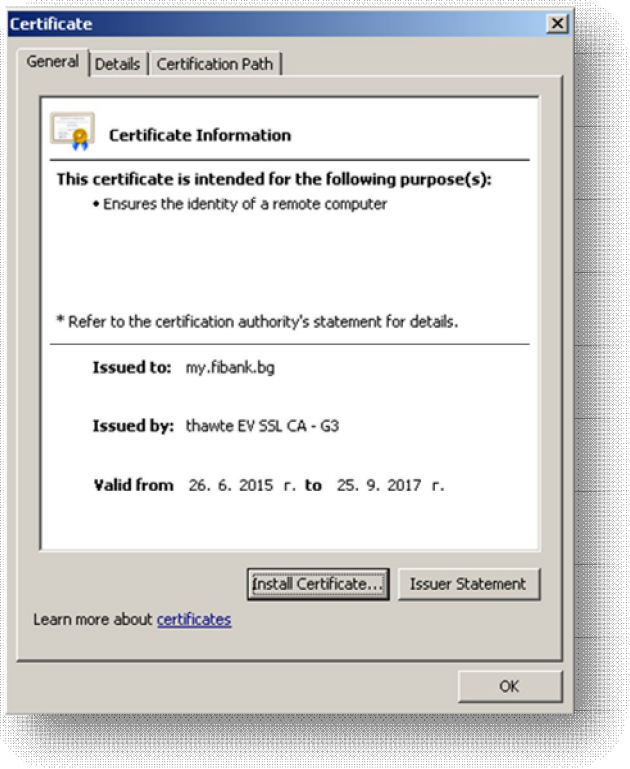


Mozilla Firefox

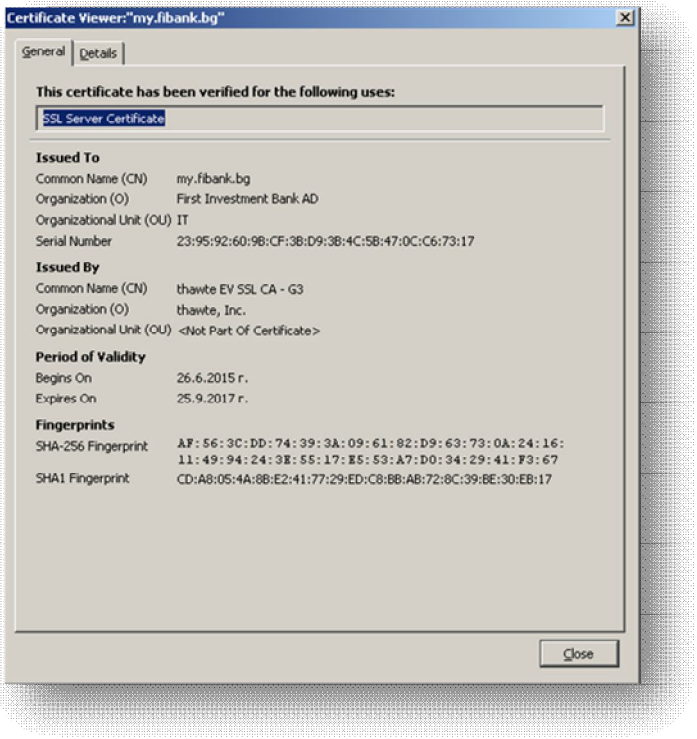
Като кликнете върху него, ще получите информация за сървърния сертификат на страницата, който задължително трябва да е издаден на /Issued to/ my.fibank.bg.

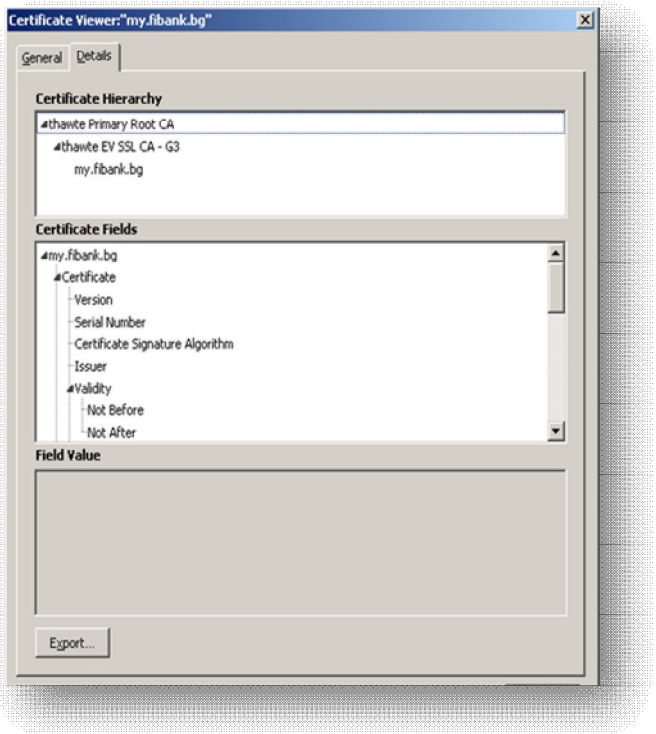
MS Internet Explorer





Mozilla Firefox





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

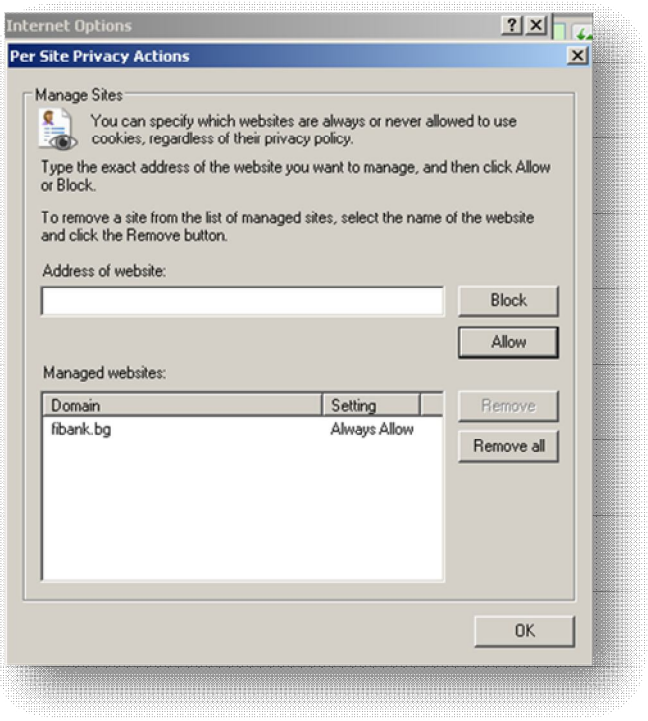
- Препоръчителни настройки на браузера при работа с Моята Fibank:

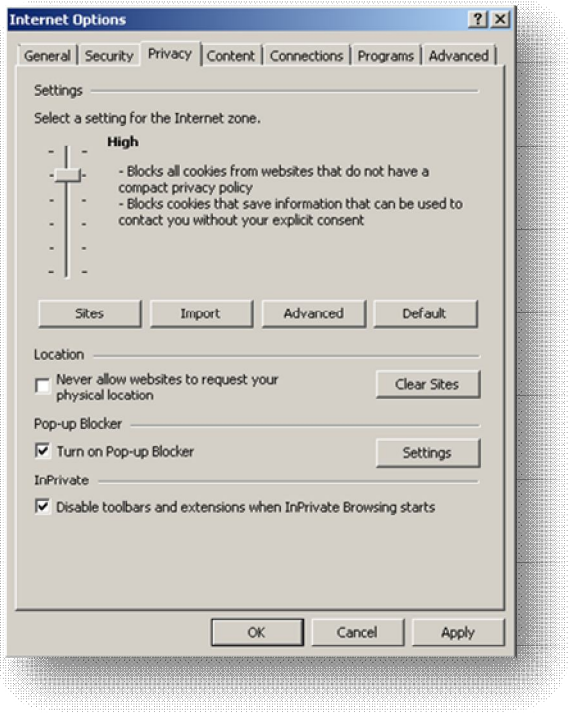
- Изключвайте всички опции на браузера, които автоматично запомнят и дописват уеб адреси, потребителски имена и пароли.

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

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

Пример:
В 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.





Препоръки за сигурност за Мобилното приложение „My Fibank”

- Мобилното приложение може да изтеглите от специализираните мобилни приложения за смарт устройства – телефони, таблети и др. Приложенията са достъпни за операционните системи Android и iOS;

- Минималните изисквания за версия на операционна система са Android OS v.4.0 и IOS 7.0;

- Fibank разпространява приложенията за смарт устройствата само чрез официалните маркети. Използвайте за инсталиране на приложенията Google Play (за Android) и iTunes (за iOS). Бутони за дотъп до Google Play и iTunes са достъпни и на уебсайтовете на Fibank и Моята Fibank на адреси www.fibank.bg и https://my.fibank.bg;

За паролата:

- Достъпът до мобилното приложение “My Fibank” се извършва с персоналното потребителско име и паролата, които ползвате и за стандартното електронно банкиране “Моята Fibank”. За допълнителна сигурност приложението не запаметява Вашата парола за достъп;

- Запомнете Вашата парола и ПИНт код и не ги записвайте в паметта на мобилния телефон, компютъра или на хартиен носител;

- Сменяйте периодично Вашата парола/ПИНт код за достъп;

- От съображения за сигурност не използвайте за парола някое от следните: име и рождена дата; поредица от числа/букви в ред (12345,abcd и други), повторение на знаци като ааа111;

- Използвайте т.н. „силна” парола, която да съдържа комбинация от главни, малки букви и цифри – поне 8 символа;

- Не предоставяйте Вашето потребителско име, пароли и ПИНт код на други лица, включително и на членове на семейството;

- Не използвайте една и съща парола за достъп/ПИНт до различни акаунти за електронно банкиране, имейли и други;

- Всеки път след приключване на работа с мобилното приложение „My Fibank” излизайте през менюто „Изход от профила” и затваряйте приложението.

За работа със смарт устройството:

- Обмислете поставянето на допълнителна защита на смарт устройството като: парола за отключване, разпознаване на лицеви черти, пръстов отпечатък, жестове и други в зависимост от модела и функционалностите на мобилното устройство. По този начин ще увеличите сигурността си при физическа кражба на устройството;

- Не предоставяйте мобилното устройство на трети лица;

- При загуба/кражба на мобилното устройство се свържете с Банката за блокиране на регистрацията Ви за Мобилното приложение;

- При съмнение за хакерска атака и кражба на лични данни, включително пароли/ПИНт, потребителско име, уведомете своевременно Банката ;

- Fibank Ви уверява, че не изисква от своите клиенти кодове за достъп до услуги, пароли, номера на банкови карти или друга конфиденциална информация чрез електронна поща;

- Инсталирайте антивирусен софтуер, предоставен от надеждни производители на антивирусни програми и използвайте официалните маркети за инсталирането му;

- Не инсталирайте и не използвайте софтуер/приложения със съмнителен произход;

- Винаги актуализирайте операционната система на смарт устройството до последната възможна. Чрез тези актуализации производителите отстраняват откритите уязвимости в по-ранните версии на системата. Изпълнявайте стриктно инструкциите на производителя;

- Не банкирайте активно от смарт устройства, които са с права на супер потребител (т.нар root) или с разширени права (т.нар jailbreak). Получаването на администраторски права предоставя възможност от злонамерени лица да получат пълен и неоторизиран достъп до цялото Ви устройство;

- Деактивирайте регистрацията на мобилното приложение от всички устройства, от които вече не работите. Ако има мобилни смарт устройства, на които сте инсталирали предишни версии на мобилното приложение и вече не работите с тях поради преинсталация на приложението или друга причина, деактивирайте тези устройства по един от определените от Банката начини.

За да заявите издаване на дигитална карта, е необходимо да:

- сте клиент на Fibank с активно банкиране в Мобилното приложение My Fibank и регистрирано мобилно устройство;
- да имате издадена дебитна или кредитна карта от Fibank;
- мобилният Ви телефон да:

  - поддържа NFC;

  - да е с лицензирана операционна система Android не по-малка от версия от 4.4;

  - да фигурира в списъка с одобрени и сертифицирани апарати от MasterCard поддържащи HCE елемент.

Host card emulation

Заявката на дигиталната карта се осъществява от мобилния Ви телефон с включено Мобилното приложение на Банката в няколко лесни стъпки.

Функции на приложението, в полза на сигурността:

- През меню „Настройки”, „Времетраене на сесията” променяйте периода на продължителност на работата Ви в приложението в зависимост от справките/операциите, които ще желаете да осъществите. Не поставяйте неоснователно голямо времетраене;

- Използвайте меню „Настройки”, „Политика на потвърждаване” и определете настройката с най-висока степен на сигурност. Fibank препоръчва използването на Токън устройство за извършване на всички видове операции, дори и на тези, за които не се изисква потвърждение с Токън устройство.

- От съображение за сигурност, за извършване на активни банкови операции през мобилното приложение „My Fibank” е необходимо да регистрирате своето смарт устройство, както и всяко ново смарт устройство, по определените от Банката начини.