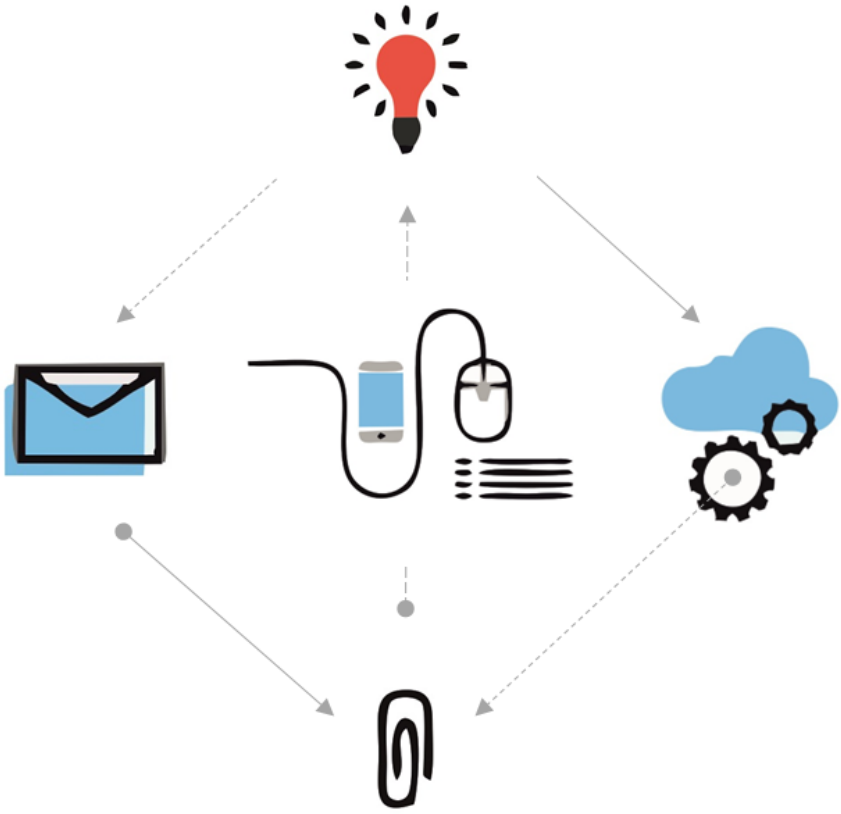


# Мерки за  сигурност

при ползване на електронното банкиране и Мобилното приложение “Моята Fibank”

05/2025 г.

## Уважаеми клиенти,

Първа инвестиционна банка (Fibank, Банката) Ви осигурява високо ниво на защита и сигурност при достъп и използване на електронното банкиране и Мобилното приложение „Моята Fibank" (My Fibank), за което се изисква да се запознаете и да спазвате настоящите Мерки за сигурност, които включват:

Съдържание

## ОСНОВНИ ПРИНЦИПИ И ПРЕПОРЪКИ

1. Сменете Вашата парола след първоначален вход в електронното банкиране или Мобилното приложение "Моята Fibank".

2. Използвайте т.нар. „силна" парола, която да съдържа комбинация от главни, малки букви, цифри, специални символи и да бъде с минимална дължина поне 8 символа. 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 aaa111. Сменяйте периодично Вашата парола за достъп.

3. Не използвайте една и съща парола за достъп до различни платформи и регистрации за електронно банкиране, имейл, социални мрежи и други.

4. Променяйте периодично 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.

5. Не предоставяйте потребителското си име, паролата, Token устройството и мобилното си устройство на трети лица. Ако е необходим достъп на член на семейството Ви/служител на фирмата Ви, направете отделна регистрация за него в електронното банкиране - той ще получи собствено потребителско име и парола за достъп.

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

7. 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", както и искане за предоставяне на данни от картите Ви, не предприемайте действия и незабавно уведомете Банката.

8. При промяна на представляващите и/или упълномощените лица, изтичане срока на упълномощаване или оттегляне на пълномощни, уведомявайте Банката своевременно.

9. При преустановяване на работата в „Моята Fibank" или оставяне на компютъра Ви без надзор, използвайте бутон "Изход" за прекратяване на сесията. Затворете и браузера, който сте използвали.

10. Използвайте антивирусна програма на компютъра, от който ползвате „Моята Fibank" и следете за нейното обновяване. Инсталирайте и използвайте анти-спайуеър софтуер, софтуер за филтриране на пощата и актуална персонална или корпоративна защитна стена (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 файлове от електронната поща или сваляте софтуер със съмнителен произход.

**11.** Използвайте максимално актуализирана операционна система и софтуерни продукти. Не използвайте Бета - версии на операционната система и/или на софтуерните продукти.

**12.** Обновявайте 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.

**13.** Не ползвайте „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 и wi-fi мрежата в дома си чрез парола.

**14.** Редовно и внимателно преглеждайте получаваната от Вас информация. Ако получите съобщение или уведомление за извънредна промяна в начина на въвеждане на средствата Ви за достъп и идентификация в „Моята Fibank“, както и искане за предоставяне на данни от картите Ви, не предприемайте действия и незабавно уведомете Банката на обявените телефони:

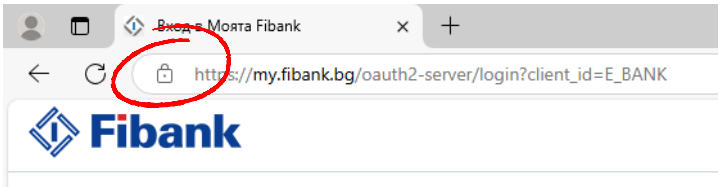
**0700 12 777**
**+359 2 800 2700**
**+ 359 2 818 0003**

**15.** 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 подсигурява от TLS протокола.

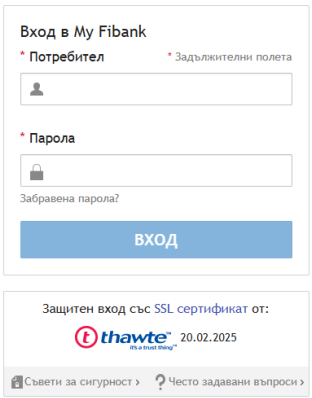
**16.** За максимална степен на сигурност използвайте последна, официална версия на браузърите.

**17.** Интернет страницата на „Моята Fibank“ се идентифицира /представя/ пред клиентите със сървърен сертификат, издаден от Thawte EV RSA 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**:

**Microsoft Edge**




Допълнително на главната страница има лого на thawte.com за онлайн проверка на автентичността на домейна на „Моята Fibank“.



**18.** Препоръчителни настройки на браузера при работа с „Моята Fibank“:

а) изключвайте всички опции на браузера, които автоматично запомнят и дописват уеб адреси, потребителски имена и пароли.

б) периодично изтривайте историята на търсене /временни файлове, cookies и други съхранени елементи/.

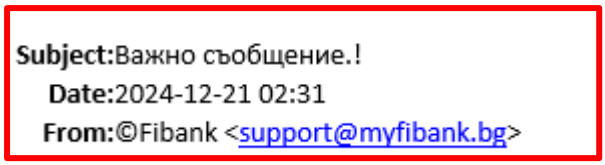
в) препоръчваме Ви да разрешите cookies („бисквитки“) само на проверени от вас страници, между които и за https://my.fibank.bg.

## МЕРКИ ПРИ ЗАПЛАХИ ТИП ФИШИНГ (PHISHING)

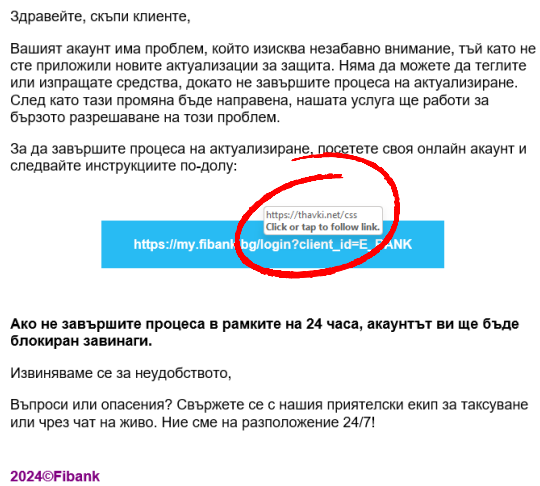
**19.** При съмнителни имейл съобщения (т.нар. phishing), получени на Вашата електронна поща, подходете с внимание. Фишингът (phishing) представлява опит за измама, при който злонамерени лица умишлено подвеждат потребителите да разкрият лична информация, средства за достъп и идентификация в „Моята Fibank“ или друга конфиденциална информация, да отварят линкове, или да въвеждат пароли, потребителско име, или изпратени на телефона като съобщение еднократно валидни кодове и т.н. При успех, те могат да проникнат в профила Ви за електронно банкиране, което може да доведе до източване на средства или други негативни последици.

а) **Особености на измамните (phishing) имейли**

- често изискват лична информация за различни цели (напр. по технически причини, като съобщения за спрян профил (акаунт), неактивен профил, актуализиране на данни в банката, подновяване на услуги, потвърждение на профил за банкиране, актуализиране на данни, добавяне на защита и др.). **Fibank никога не изисква подобна информация**.
- дори ако полето за подател „От:/From:“ показва Fibank, това не гарантира, че полученият имейл е от Банката.




- Обикновено съдържат **несъответствие** между домейна на подателя и този в линковете.




- съдържат предупреждения от „спешен порядък“, които могат да Ви алармират за потенциална измама, като „Профилът е блокиран“, „Вашият акаунт има проблем“, „Ако

не завършите процеса в рамките на 24 часа, акаунтът ви ще бъде блокиран завинаги“, „Важно съобщение“, „Потвърдете акаунта си:“ „Важна стъпка за продължаване на използването на услугите на Fibank“.

- съдържат линкове за въвеждане и потвърждаване на информация от личен и банков характер. Не кликвайте на тези линкове, Fibank никога няма да изиска от Вас въвеждане на информация в линк, изпратен чрез съобщение. Уведомленията от Банката могат да съдържат само документи, които се отварят без въвеждане на персонална информация, например при промени в Тарифата и общите условия.

б) **Прикачени файлове:**

- Не отваряйте и не запазвайте прикачени файлове от съмнителни електронни съобщения.

в) **Изисквания за конфиденциална информация:**

- Първа инвестиционна банка АД **не изисква** изпращане на ПИН-ове, пароли или друга конфиденциална информация чрез електронна поща.
- **Не изпълнявайте инструкции** от съобщения, които искат обаждане на посочен телефон за споделяне на идентификационни данни.

**20.** 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.

## ДОПЪЛНИТЕЛНИ МЕРКИ ПРИ МОБИЛНОТО ПРИЛОЖЕНИЕ “MY FIBANK”:

**21.** За получаване на достъп до Вашия профил в Мобилното приложение “My Fibank” е необходимо да активирате мобилното приложение на Вашето мобилно устройство, чрез спазване на стъпков процес определен от Банката, при който се прилага задълбочено установяване на идентичността.

**22.** Мобилното приложение “My Fibank” може да намерите и изтеглите на Вашето мобилно устройство (мобилен телефон, таблет и др.) от специализираните официални магазини за мобилни приложения – Google Play (Android), AppStore (iOS/iPad OS) и AppGallery (HarmonyOS). Минималните изисквания за версия на операционна система са Android OS v.8.0 и iOS 16.0.

**23.** Запомнете Вашия ПИНт код и не го записвайте в паметта на мобилния телефон, компютъра или на хартиен носител.

**24.** За по-голяма сигурност препоръчваме да използвате биометрични данни - Пръстов отпечатък (Fingerprint), Лицево разпознаване (FaceID), за достъп и идентификация, и потвърждение на електронни операции чрез Мобилното приложение.

**25.** Не запазвайте и не съхранявайте биометрични данни на други лица в Мобилното устройство.

**26.** Сменяйте периодично Вашия ПИНт код за достъп и идентификация.

**27.** Не задавайте твърде лесен ПИНт код, като избягвате шаблонни комбинации от цифри или цифри свързани с Вашата рожденна дата и година на раждане.

28. Прочитайте внимателно текстовете на съобщенията, които Банката ви изпраща под формата на SMS или push известия. Преди да въведете получен от Банката код, внимателно се запознайте с текста на съобщението, съдържащ информация за действието, за което кода се отнася. Не въвеждайте кода, ако не разпознавате като свое действието, за което кодът се отнася. Преди да потвърдите превод, проверявайте внимателно съобщенията съдържащи информация за сумата и валутата на превода, сметките на наредител и получател на средствата. При съмнение или получаване на съобщение, съдържащо действие, което не разпознавате, не извършвайте каквито и да е действия за потвърждаване, за предоставяне на кодове и информация. Незабавно се свържете с Fibank.

29. От съображения за сигурност, Банката информира клиентите си, чрез уведомителни съобщения по e-mail и SMS, при всяко активиране на Мобилното приложение на ново устройство. Бъдете бдителни! В случай че получите съобщение за активиране на Мобилното Ви приложение на ново устройство, а Вие не сте инициирали подобна операция, незабавно се свържете с Банката на посочените по-горе, както и в Общите условия за електронно банкиране “Моята Fibank” телефони.

30. През меню „Профил”, „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.

31. Използвайте меню „Профил”, „Политика на потвърждаване” и определете настройката вход и извършване на всички видове операции.

32. Използвайте меню „Известия“ за активиране на получаването на електронни съобщения „push notification” от уведомителен характер с данни за платежни операции и/или справочна информация, за да бъдете винаги информирани и незабавно да реагирате при съмнение за подозрителни активности с профила ви.

## РАБОТА С МОБИЛНО УСТРОЙСТВО

33. Поставете допълнителна защита на мобилното си устройство като: парола за отключване, лицево разпознаване, 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.

34. Не предоставяйте мобилното устройство за ползване на трети лица в т.ч. деца, родители, съпрузи, включително за ползване на функционалността за биометрични данни.

35. При загуба/кражба на мобилното устройство се свържете с Банката за блокиране на регистрацията Ви за електронното банкиране “Моята Fibank” и Мобилното приложение “My Fibank”.

36. При съмнение за хакерска атака и кражба на данни, включително пароли/ПИНт, потребителско име, уведомете незабавно Банката.

37. Не инсталирайте и не използвайте софтуер/приложения със съмнителен произход.

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

**39.** Не банкирайте активно от мобилни 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;

## ОПАСНОСТИ В ЕРАТА НА ИЗКУСТВЕНИЯ ИНТЕЛЕКТ

**40.** С развитието на технологиите злонамерените лица използват нови методи за социално инженерство, включително манипулирани обаждания и аудио-визуални съобщения.

**41.** Бъдете внимателни при получаване на обаждания, които звучат странно или използват роботизирани или неестествени гласове. Съвременни технологии като „дийпфейк" позволяват имитация на гласове с висока точност. Ако получите обаждане, което изисква конфиденциална информация или достъп до вашите акаунти, прекъснете връзката и се свържете директно с Банката.

**42.** Както бе посочено по-горе, Fibank не изисква от своите клиенти пароли, потребителски идентификатор, кодове за достъп до услуги (например до „Моята Fibank"), PIN-кодове, номера на банкови карти или друга конфиденциална информация. С напредването на технологиите, злонамерени лица използват напредналите технологии и средства на изкуствения интелект, за да заблудят потенциалните жертви. Използвайки аудио-визуални материали от интернет, като снимки и видеа от официални събития, злонамерените лица могат да пресъздадат правдоподобно видео на близък или официално лице от Банката, напр. Изпълнителен Директор, в което той/тя изисква от потребителите да предоставят информация. Стандартно се упражнява натиск, чрез създаване на усещане за спешност. Въпреки че изкуственият интелект генерира почти перфектни подобия на лица, той не е перфектен и потребителите могат да разпознаят видео направено с изкуствен интелект.

**43.** Аудио-визуалните материали направени с изкуствен интелект с образите на специфични лица имат в себе си така наречените „артефакти". Това са неестествени движения и изражения по лицето на човека, чиято самоличност е присвоена. Артефакти са и още аномалии с броя пръсти на ръцете. Обикновено моделите за изкуствен интелект създаващи такива материали изпитват трудности с тези тънкости, като изкривяват усмивки или поставят повече или по-малко пръсти на ръцете, ако визуалния материал включва кадри с тях.

**Настоящите Мерки за сигурност** са публикувани на корпоративната страница на Банката в секция Дистанционно банкиране/ Препоръки и указания. Достъпни са и от началния екран за вход в електронното банкиране „Моята Fibank" и в профила Ви в Мобилното приложение „MyFibank", като подлежат на актуализиране, за което следва периодично да се запознавате с тях.

**Бъдете информирани.**