Безопасность системы «Мобильный банкинг» ПАО «МТС-Банк»

Система дистанционного банковского обслуживания (ДБО) **Мобильный банкинг** ПАО «МТС-Банк» (далее – Система) предоставляет возможность управлять денежными средствами на Ваших банковских счетах, открытых в Банке, посредством мобильного устройства (мобильного телефона, смартфона, планшетного компьютера).
Для обеспечения защиты от несанкционированного доступа и проведения платежей, Система включает в себя следующие средства доступа:
Логин – уникальная последовательность символов, позволяющая Вас идентифицировать;
Пароль – секретный набор символов, известный только Вам, используемый для входа в систему;
Сеансовый ключ (далее –SMS-ключ) –одноразовый цифровой код, аналог собственноручной подписи (АСП) Клиента, используемый совместно со Средствами доступа (логин и пароль), если иное не предусмотрено положениями настоящих Условий, для подтверждения операций, проводимых в Системе ДБО.
Операции в Системе МБ на сумму до 10 000 рублей (включительно) подтверждения не требуют.

Правила безопасности для Клиента:
1. Установку приложений Системы совершайте только по ссылкам на официальном сайте Банка или авторизованных магазинах приложений (App Store, GooglePlay, Windows Phone Store). Все остальные источники получения приложения не являются официальными, и Банк не несет ответственности за последствия установки приложений из данных источников.
2. Необходимо наличие на Вашем мобильном устройстве антивирусного программного обеспечения с регулярно обновляемыми базами. Для платформы Android рекомендуем к использованию бесплатные приложения антивирусов CM Security, Kaspersky Internet Security, а также 360 Security.
3. Своевременно ставьте в известность ПАО «МТС-Банк» о смене номера телефона мобильной связи, который клиентом был предоставлен в ПАО «МТС-Банк» для получения услуги «мобильный банкинг», в том числе, на который происходит информирование об операциях по счету клиента.
4. Не переходите по ссылкам, приходящим из недостоверных источников, в том числе на известные сайты.
5. Не скачивайте на мобильное устройство приложения из непроверенных источников.
6. Не передавайте мобильное устройство и платежную карту (карты) для использования третьим лицам, в том числе родственникам.
7. Не сообщайте третьим лицам, в том числе работникам ПАО «МТС-Банк», ПИН-код платежной карты и контрольный код, указанный на оборотной стороне платежной карты (CVV/CVC), номер счета, одноразовые коды подтверждения; при наличии подозрения, что такие данные стали известны третьему лицу, необходимо сообщить об этом в ПАО «МТС-Банк» по контактным данным, указанным на официальном сайте (http://www.mtsbank.ru/).
8. Не сообщайте конфиденциальные данные посторонним лицам (паспортные данные, логин, пароль и пр.).
9. Регулярно проводите обновление приложений и операционной системы Вашего мобильного устройства с официальных источников фирм разработчиков.
10. На устройстве не рекомендуется проводить операцию root и jailbreak. Это значительно снизит уровень безопасности Вашего мобильного устройства к угрозам заражения вредоносными программами.
11. Рекомендуем установить парольную защиту на Ваше мобильное устройство.
12. Завершайте работу в мобильном приложении нажатием кнопки «Выход».
13. Не храните средства доступа в Систему на своем мобильном устройстве (в заметках, напоминаниях, SMS, и пр.).
14. Используйте сложные пароли доступа, избегая легко угадываемых вариантов.

15. Отключите в настройках Вашего мобильного устройства (iPhone) возможность использования голосового помощника Siri на заблокированном экране.
16. Следите за своими операциями. Выписка по картам и счетам, полученная через систему, позволит Вам своевременно обнаружить и оперативно известить Банк об имеющихся несоответствиях.

Важно! ПАО «МТС-Банк» не высылает писем по электронной почте или SMS с целью уточнить персональную информацию о Клиенте.

Признаки того, что Ваши данные могли стать известными третьим лицам:

- Появление в списке платёжных документов, которые Вы не формировали;
- Получение SMS уведомлений о платежах, которые Вы не совершали.

Если Вы утратили средства доступа к Системе (логин, пароль), незамедлительно обратитесь в Службу поддержки клиентов для их блокировки:

- для звонков по России: 8(800)250-05-20
- для звонков из-за рубежа: +7(495)777-000-1
- по короткому номеру для абонентов МТС 0515

Восстановить доступ к Интернет- или Мобильному банку вы также можете с помощью любого банкомата и терминала Банка, а также в любом офисе ПАО «МТС Банк».

Приложение системы Мобильный банкинг может запрашивать следующие разрешения на устройстве:

1. Использование телефона – для совершения звонка Клиента в Банк.
2. Использование сетевых служб устройства – для корректного доступа к серверам Банка.
3. Использование сведений об устройстве – для сохранения истории действий Клиента.
4. Доступ к браузеру – для отображения внешних страниц интернет.
5. Использование библиотеки мультимедиа и камеры для изменения пользовательского фото в приложении.
6. Интернет – для загрузки данных.
7. Статус сети – для проверки возможности загрузки данных.
8. Местоположение – для получения данных о ближайших географических объектах (в целях предоставления рекламных и прочих информационных услуг Банк может сохранять информацию о местоположении, полученную с абонентского устройства Клиента)
9. Контакты – для выбора номера телефона из списка контактов при оплате сотовой связи.
10. Чтение и запись календаря – для установки напоминаний по ближайшим платежам по кредиту
11. СМС – для улучшения удобства использования подтверждения операций разовыми паролями.
12. Просмотр конфигураций Google – для корректной работы приложения.
13. Управление функцией вибросигнала – для определения встряхивания телефона.
14. Просмотр сетевых подключений - для проверки доступности сети перед выполнением запросов.
15. Использование сканера отпечатка пальцев – для возможности авторизации в приложении с использованием отпечатка пальцев.
16. Передача карты ПАО «МТС-Банк» по согласию Клиента в Apple Wallet, Android Wallet, Samsung Wallet.
17. В целях обеспечения безопасности финансовых транзакций передавать информацию о действиях клиента, совершенных в приложении, в ООО «Кибертоника» по адресу https://p.cybertonica.com