Безопасность системы Мобильное приложение «МТС Банк Бизнес Клиент»» ПАО «МТС-Банк»

Мобильное приложение «МТС Банк Бизнес Клиент» (далее – Система) предоставляет доступ к системе «Клиент-банк» для юридических лиц и индивидуальных предпринимателей 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 и пароль – секретный набор символов, известный только клиенту, используемый для входа в Систему;
SMS-код - уникальная последовательность символов, предназначенная для подтверждения операций в Мобильном приложении, направленная ПАО «МТС-Банк» (далее - Банк) в виде SMS-сообщения на номер мобильного телефона, зарегистрированный в Банке для целей получения SMS-кода.

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 Банк о смене номера телефона мобильной связи, зарегистрированный в Банке.
4. Не переходите по ссылкам, приходящим из недостоверных источников, в том числе наизвестные сайты.
5. Не скачивайте на мобильное устройство приложения из непроверенных источников.
6. Не передавайте мобильное устройство для использования третьим лицам, в том числе родственникам.
7. Не сообщайте третьим лицам, в том числе работникам Банка номер счета, одноразовые коды подтверждения; при наличии подозрения, что такие данные стали известны третьему лицу, необходимо сообщить об этом в Банк по контактным данным, указанным на официальном сайте (http://www.mtsbank.ru/).
8. Не сообщайте конфиденциальные данные посторонним лицам (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! 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: **8-800-250-01-99**

Восстановить доступ к Сервису вы также можете в любом офисе Банка, обслуживающем корпоративных клиентов .

Приложение Системы 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. Просмотр сетевых подключений - для проверки доступности сети перед выполнением запросов.