Меры безопасности при использовании мобильного приложения «Сбербанк Бизнес Онлайн»

В мобильных приложениях «Сбербанк Бизнес Онлайн» (далее – СББОЛ) используются современные механизмы и средства обеспечения информационной безопасности, направленные на то, чтобы сделать работу с системой максимально удобной при поддержании высокого уровня безопасности. Вместе с тем, соблюдение приведенных рекомендаций позволит максимально безопасно работать с Системой и свести риски мошенничества и, как следствие, финансовые потери к минимуму.

- Пароли, кодовые слова, одноразовые пароли для входа в мобильное приложение СББОЛ или полнофункциональную версию – это Ваша личная конфиденциальная информация, ни при каких обстоятельствах не раскрывайте их никому, включая сотрудников Сбербанка России.
- Не вводите в мобильном приложении или где-либо еще ваш пароль к полнофункциональной версии СББОЛ, мобильное приложение его не использует. Для аутентификации в мобильном приложении используется онлайн ПИН-код, назначенный Вами при его активации.
- Первоначальный экран мобильного приложения при втором и последующих запусках мобильного приложения содержит только поле ввода онлайн ПИН-кода. В случае если на данном экране от Вас требуется ввод любой другой персональной информации (номеров банковских карт, мобильного телефона, других личных данных), следует прекратить использование услуги и связаться с Банком.
- Не сохраняйте Ваш онлайн ПИН-код на мобильном телефоне, на которых Вы запускаете мобильное приложение.
- Не сохраняйте Ваш онлайн ПИН-код в текстовых файлах на компьютере либо на других электронных носителях информации, т.к. при этом существует риск его кражи и компрометации.
- При любых подозрениях на компрометацию онлайн ПИН-кода посторонними лицами (в т.ч. представившимися сотрудниками Банка), следует незамедлительно обратиться в Банк.
- Не оставляйте свой мобильный телефон без присмотра, чтобы исключить несанкционированное использование мобильного приложения.
- Используйте антивирус для мобильного телефона и своевременно устанавливайте на него обновления вирусных баз.
- Своевременно устанавливайте доступные обновления операционной системы и приложений на ваш телефон.
- Не взламывайте свой телефон (например, через Jailbreaking), так как это отключает защитные механизмы, заложенные производителем мобильной платформы. В результате ваш телефон становится уязвимым к заражению вредоносным ПО.
- Не переходите по ссылкам и не устанавливайте приложения/обновления безопасности, пришедшие по SMS/электронной почте, в том числе от имени банка. Помните, что банк не рассылает своим клиентам ссылки или указания на установку приложений через SMS/MMS/Email - сообщения.
- Установите парольную защиту на телефоне. Данная возможность доступна для любых современных моделей телефонов.
- При подтверждении операций одноразовым SMS-паролем необходимо контролировать соответствие реквизитов операции и реквизитов в полученном sms-сообщении.

- Завершайте работу с мобильным приложением через завершение сессии (кнопка «Выход»).
- При потере/смене номера телефона обязательно сообщите об этом в Банк.
- В случае если у Вас неожиданно перестала работать sim-карта телефона, следует оперативно обратиться к своему оператору сотовой связи для блокировки абонентского номера и замены sim-карты, а также обратиться в Банк для выявления возможных несанкционированных операций.
- При утрате мобильного телефона, на который установлено мобильное приложение, Вам следует срочно обратиться к своему оператору сотовой связи для блокировки sim-карты, заблокировать ваше мобильное приложение при помощи WEB-интерфейса “Сбербанк Бизнес Онлайн”, а также обратиться в Банк для выявления возможных несанкционированных операций.
- Не используйте мобильный телефон для доступа к полнофункциональной версии СББОЛ, для этого существует мобильное приложение, разработанное банком.
- Регулярно контролируйте состояние своих счетов и незамедлительно сообщайте сотрудникам Банка обо всех подозрительных или несанкционированных операциях.