Приложение № 3
к Правилам дистанционного банковского обслуживания
физического лица в АКБ «Трансстройбанк» (АО)

Памятка Клиента

Уважаемый Клиент!

Заключив Договор дистанционного банковского обслуживания физического лица в АКБ «Трансстройбанк» (АО), Вы стали пользователем Системы дистанционного банковского обслуживания. Пожалуйста, внимательно прочтите эту Памятку.

Эта Памятка написана для того, чтобы Ваши финансовые средства оставались только Вашими!

Интернет предоставляет замечательные возможности по удаленному управлению своими финансами.

Но, вместе с тем, нужно всегда помнить о рисках, связанных с работой через Интернет.

Доступ в Систему дистанционного банковского обслуживания возможен через сеть Интренет посредством следующих браузеров (веб-обозревателей) Internet Explorer, Opera, Mozilla FireFox, Google Chrome, Safari или через мобильное приложение, которое размещено в App Store или Google Play.

Вы должны самостоятельно настроить все аппаратные и программные средства для обеспечения возможности работы с сетью Интернет по протоколам http, https. Специалисты Банка не оказывают консультации по данным вопросам.

ЗАПОМНИТЕ:

- Для обеспечения защиты конфиденциальной информации на программном уровне на Вашем компьютере должно быть установлено регулярно обновляемое лицензионное антивирусное и иное программное обеспечение, обеспечивающее безопасность компьютера при работе в сети Интернет
- При входе на страницу авторизации Вам необходимо убедиться в том, что Вы находитесь на Корпоративном интернет-сайте Банка https://online.transstroybank.ru и соединение является защищенным. То есть в адресной строке Интернет-браузера отображается признак защищенного соединения https:// (обязательно символ s после http) В браузере появляется изображение замка (справа или слева от адресной строки, либо справа вверху/внизу браузера). Кликнув по замку, можно убедиться в подлинности сертификата. Сертификат удостоверяет, что этот адрес принадлежит именно АКБ «Трансстройбанк» (АО)
- Внимательно следите за тем, что адрес в браузере именно такой https://online.transstroybank.ru а не «похожий» на него https://online.transstroubank.ru или https://online.transstr0ybank.ru
- Логин и пароль держите в секрете, не пересылайте по почте или SMS
- Пароль не должен быть простым (123456, qwerty и др.)
- Не сообщайте пароль никому, в том числе специалистам, обслуживающим компьютер
- Регулярно меняйте пароль, не реже 1 раза в месяц
- Не используйте одинаковые пароли для Системы ДБО и для других сервисов @mail.ru, @gmail.com и др.
- Пароль необходимо поменять в случае подозрений на компрометацию. Рекомендуется это сделать даже после работы с Системой ДБО на чужом компьютере
- Пароль необходимо поменять в случае обнаружения каких-либо вредоносных программ. Сделать это нужно с другого компьютера
- Не используйте на своем компьютере любые средства удалённого (дистанционного) доступа, которые обычно практикуют IT-специалисты для удалённой (дистанционной) поддержки (TeamViewer и др.). Заблокируйте возможность использования таких средств с помощью файрвола (программного и/или аппаратного)

- Защитите свой мобильный телефон кодом блокировки экрана
- Не устанавливайте на мобильный телефон, на который Банк отправляет SMS-сообщения с подтверждающим одноразовым паролем, приложения, полученные от неизвестных Вам источников. Помните, что Банк не рассылает своим клиентам ссылки или указания на установку приложений через SMS/MMS/Email сообщения
- Для входа в Систему ДБО требуется вводить только Ваш Логин и Пароль, а также Одноразовый пароль для входа из SMS-сообщения. Ваш номер мобильного телефона, номер Вашей банковской карты или код CVV2/CVC2 для входа или дополнительной проверки при авторизации в Системе ДБО не требуется, и указывать такие данные не нужно! (за исключением случая заключения Договора способом, предусмотренным пунктом 3.1.2 Правил)
- При утрате мобильного телефона, на который Банк отправляет SMS-сообщения с подтверждающим одноразовым паролем, Вам следует незамедлительно обратиться к своему оператору сотовой связи и заблокировать телефонную SIM-карту
- Банк не запрашивает у Клиента значения средств авторизации по телефону, по электронной почте либо иным способом. Банк не рассылает Клиентам электронные сообщения, содержащие ссылку на корпоративный Интернет-сайт Банка, с просьбой подтвердить значения средств авторизации. При поступлении Вам подобных электронных сообщений якобы от Банка Вы ни в коем случае не должны сообщать значения средств авторизации, запрашиваемые у Вас под предлогом уточнения сведений либо под иным предлогом, и нажимать на ссылки, содержащиеся в сообщении.