

Уважаемые Клиенты!

Напоминаем Вам об основных мерах обеспечения безопасности при работе с системой дистанционного банковского обслуживания «Банк-Клиент» (далее система ДБО Банка):

1. Необходимо использовать компьютер только для целей осуществления электронных платежей в системе ДБО Банка. Не следует использовать компьютер для посещения сайтов в сети Интернет, а также для получения писем с неизвестных адресов электронной почты – это может привести к заражению компьютера вирусами. Установите и настройте персональный межсетевой экран (firewall) на компьютере с системой ДБО Банка. Разрешите доступ с компьютера только на необходимые для работы IP-адреса (сервер системы ДБО Банка, серверы обновления операционной системы и антивируса).
2. Убедитесь, что Ваш компьютер не заражен вирусами. Установите и периодически проверяйте корректность работы антивирусного программного обеспечения. Ежедневно обновляйте антивирусные базы. Обращаем Ваше внимание, что действие вирусов может быть направлено на запоминание и передачу третьим лицам информации о Ваших паролях и ключах электронной подписи.
3. Используйте лицензионное программное обеспечение, полученное только из проверенных и надежных источников. Для устранения существующих уязвимостей оперативно устанавливайте последние пакеты обновлений (Service Packs) и актуальные патчи безопасности для операционной системы и прикладного программного обеспечения. Удалите с компьютера программное обеспечение, не связанное с подготовкой и осуществлением электронных платежей в системе ДБО Банка.
4. Необходимо ограничить доступ к компьютеру, с которого осуществляется подключение к системе ДБО Банка. Для этого установите компьютер в недоступном для посторонних лиц месте. Желательно, чтобы это помещение закрывалось на ключ. Постарайтесь разместить экран монитора таким образом, чтобы изображение на нем не было заметно посторонним. Иногда одним ограничением физического доступа снимаются многие проблемы с безопасностью.
5. Необходимо установить пароль на доступ к компьютеру. Крайне желательно установить на рабочий стол «экранную заставку» со временем начала работы не более 5 минут (т.е. если ответственный сотрудник не работает за компьютером более 5 минут – компьютер включает «экранную заставку»), которую можно разблокировать только после ввода пароля. Длину пароля лучше выбрать не менее 8 символов. Желательно, чтобы этот пароль нельзя было угадать, т.е. цифры вашего телефона, имена близких людей, клички домашних животных и прочие известные о Вас факты в пароле использовать не стоит. Хранение пароля в электронном виде недопустимо!
6. При первом подключении eToken необходимо изменить PIN-код и хранить его в секрете. При этом пароль не должен совпадать с паролем доступа к Вашему компьютеру.
7. Крайне внимательно относитесь к ключевому носителю, не оставляйте его без присмотра и не передавайте третьим лицам, извлекайте ключевые носители из компьютера, если они не используются для работы. Ключ должен храниться отдельно от компьютера в сейфе директора компании или у ответственного сотрудника и не должен быть доступен посторонним лицам (в том числе и сотрудникам компании, не связанным с проведением электронных платежей).
8. Не оставляйте eToken без присмотра во время работы данных специалистов с Вашим компьютером. Отправляя в ремонт компьютерное оборудование, проследите, чтобы на жестком диске компьютера не оставалось конфиденциальной информации.

9. Будьте внимательны при вводе адреса сервера системы ДБО Банка. Не переходите на сервер системы ДБО Банка по внешним ссылкам через подложные веб-сайты. Банк никогда не будет просить у Вас сообщить Ваш логин и пароль по электронной почте или каким-либо другим путём.

10. При возникновении малейших подозрений на компрометацию ключей электронной подписи, а также при утере компьютера с установленной системой ДБО «Банк-Клиент» необходимо незамедлительно информировать Банк для принятия неотложных мер по блокировке ключей электронной подписи с целью недопущения их несанкционированного использования.

Банк применяет широкий комплекс мер по обеспечению безопасности операций в системе ДБО «Банк-Клиент». Но помните, что обеспечение безопасности финансовых операций – наше общее дело!

С уважением, ПАО КБ "РусьРегионБанк"