Рекомендации по обеспечению безопасности при работе с Системой ДБО «iBank2»

В целях обеспечения безопасности при работе с Системой ДБО «iBank2» необходимо соблюдать следующие меры:

1. Подключайте USB-токен к компьютеру ТОЛЬКО в момент начала работы с интернет-банкингом, и ОБЯЗАТЕЛЬНО извлекайте его из компьютера сразу после окончания работы.
2. Не устанавливайте галочку «Запомнить пароль» для USB-токена.
3. Если USB-токен не используется - храните его в сейфе, запираемом ящике стола или другом месте с ограниченным доступом. Также ограничьте доступ к телефону, на номер которого приходят СМС с кодами подтверждения платежей.
4. При смене номера телефона или его утере незамедлительно обращайтесь в АО РОСЭКСИМБАНК для его замены на новый номер.
5. Своевременно проводите смену ключевой информации:
    - При окончании срока действия сертификата;
    - При смене ответственных лиц, имеющих право использования Системы ДБО «iBank2»;
    - При обнаружении фактов доступа неуполномоченных лиц к ключевой информации или подозрениях в том, что такой доступ мог иметь место.
6. Перед вводом SMS кода для подтверждения платежа, убедитесь, что информация, полученная в сообщении SMS, соответствует фактическим реквизитам платежа (счет, сумма, БИК и т.д.).
7. Ограничьте доступ к компьютеру, используемому для работы с Системой ДБО «iBank2», не допускайте к нему посторонних лиц.
8. Соблюдайте правила безопасной работы в сети Интернет. Не используйте компьютер, где установлена Система ДБО «iBank2» для посещения сайтов сомнительного содержания. Не используйте на данном компьютере мессенджеры.
9. Установите антивирусную программу и персональный межсетевой экран (firewall). Ежедневно обновляйте антивирусные базы.
10. Обеспечьте защиту компьютера от несанкционированного доступа за счет использования уязвимостей программного обеспечения: организуйте своевременную установку обновлений безопасности операционной системы и прикладных программ.
11. Используйте только лицензионное программное обеспечение, полученное из доверенных источников.
12. Для входа на защищенную веб-страницу Системы ДБО «iBank2» используйте только адрес https://ibank2.eximbank.ru/.
13. Внимательно контролируйте состояние Ваших расчетных счетов путем формирования выписки не реже 1 раза в день, даже если Вы не проводите платежные операции в системе. Подключите услугу SMS-информирование.
14. Не устанавливайте и не сохраняйте подозрительные файлы, полученные из ненадежных источников, скачанные с неизвестных web-сайтов, присланные по электронной почте и т.д. В случае необходимости загрузки файла, полученного из потенциально небезопасного источника, обязательно перед использованием проверьте его антивирусом.
15. Если возникло подозрение, что компьютер заражен вирусом (неадекватная реакция на действия пользователя, появляющиеся непонятные окна, получение незапрашиваемых SMS с кодом для входа или для проведения операции и т.п.) - немедленно прекратите работу в системе «iBank2», извлеките USB-токен и обратитесь к ИТ-специалисту для выяснения причин происходящего. До выяснения причин не пользуйтесь системой «iBank2»!
16. Внимательно прочитайте рекомендации по обеспечению информационной безопасности в системе дистанционного банковского обслуживания, которые являться приложением к

Условиям предоставления АО РОСЭКСИМБАНК услуги дистанционного банковского обслуживания.

Внимание!

АО РОСЭКСИМБАНК никогда не запрашивает у клиентов конфиденциальную информацию (пароли, SMS-коды, пароли для ключевого носителя)!

АО РОСЭКСИМБАНК не имеет доступа к секретным ключам клиентов. У АО РОСЭКСИМБАНК отсутствует технологическая возможность подписания документов электронной подписью от имени какого-либо клиента. В АО РОСЭКСИМБАНК хранятся только сертификаты открытого ключа электронной подписи клиентов, сформированные и переданные клиентами в Банк при подключении к Системе ДБО «iBank2». Данные сертификаты могут быть использованы только для проверки электронной подписи платежных документов, полученных от клиентов.

АО РОСЭКСИМБАНК не несет ответственности за сохранность ключевой информации клиентов (она хранится только у клиентов и только клиент является ее единственным владельцем), а также за возможный ущерб, который может понести клиент в случае исполнения АО РОСЭКСИМБАНК платежных документов, созданных неуполномоченными лицами, но подписанных действительной электронной подписью клиента.