Рекомендации по обеспечению информационной безопасности при работе в системе ДБО Интернет-банк

Уважаемый Клиент!

Безопасность работы в системе ДБО Интернет-банк обеспечена комплексом организационных и логических мер, направленных на предотвращение мошенничества и разглашения конфиденциальной информации.

Со стороны клиента безопасность работы в системе обеспечивается выполнением следующих рекомендаций:

Общие рекомендации по обеспечению безопасности при работе в Интернет

При работе в Интернет рекомендуем Вам соблюдать общие правила безопасности, применяющиеся для защиты любых данных, хранящихся на компьютерах.

1. При работе с электронной почтой не открывать письма и вложения к ним, полученные от неизвестных отправителей, не переходить по содержащимся в таких письмах ссылкам.
2. Своевременно обновлять операционную систему (установка патчей, критичных обновлений).
3. Не использовать права администратора при отсутствии необходимости. В повседневной практике входить в систему как пользователь, не имеющий прав администратора.
4. Установить и своевременно обновлять на компьютере антивирусное ПО (NOD32, AVP Kaspersky, Symantec AntiVirus и т.д.).
5. Антивирусное ПО должно быть запущено постоянно с момента загрузки компьютера. Рекомендуется полная еженедельная проверка компьютера на наличие вирусов, удаление обнаруженного вредоносного ПО.
6. Не давать разрешения неизвестным программам выходить в интернет.
7. При работе в интернет не соглашаться на установку каких-либо дополнительных программ.
8. Осуществлять информационное взаимодействие с Банком и другими кредитными организациями только с использованием средств связи (мобильные и стационарные телефоны, факсы, интерактивные WEB-порталы/сайты, обычная и электронная почта), реквизиты которых оговорены в документах, получаемых непосредственно в Банке или других кредитных организациях.

Рекомендации по обеспечению безопасности при работе в системе ДБО Интернет-банк

В сети Интернет получили широкое распространение специализированные вредоносные программы (трояны), обеспечивающие возможность похищения у пользователей финансовых интернет-систем файлов с секретными ключами ЭП и пароли, вводимые с клавиатуры. Трояны распространяются через e-mail, по каналам ICQ, Skype, через принадлежащие преступникам сайты.

Для того чтобы защитить Ваши средства, настоятельно рекомендуем использовать на компьютере, с которого осуществляется работа с системой ДБО Интернет-банк, следующий комплекс дополнительных мер безопасности:

- Подключить дополнительные средства защиты: **разовые SMS-пароли**, которые будут приходить на указанный Вами номер мобильного телефона. Пароль необходимо вводить для подтверждения входа в систему ДБО Интернет-банк и платежей, относимых системой контроля к категории потенциально рисковых.

- Настроить сервис **«SMS-уведомления об отправке платежных документов в банк»** в разделе «Безопасность». Дополнительно можно настроить **E-mail-уведомления** об отправке и исполнении документов, а также обо всех входах в Интернет-банк.
- Контролировать состояние счёта (путем просмотра выписки).
- Обращать внимание на дату и время последних входов в систему (данные фиксируются на первой странице после входа в систему, а также в специальном разделе «Безопасность -> Журнал сеансов работы»).
- При использовании смарт-ключа подключайте его только на время работы с системой ДБО Интернет-банк по окончании сеанса смарт-ключ необходимо извлечь.
- Настоятельно не рекомендуем осуществлять работу в системе ДБО Интернет-банк с компьютеров, расположенных в общественных местах (интернет-кафе, бизнес центрах отелей, игровых залах, компьютеры третьих лиц и т.д.), так как на данных компьютерах невозможно гарантировать соблюдения режима информационной безопасности (наличие антивирусных средств, отсутствие вредоносного и шпионского программного обеспечения, отсутствие программ теневого копирования и т.д.), что существенно увеличивает риск хищения Ваших идентификационных и аутентификационных данных (логинов, паролей, номера платежной карты и срока ее действия, кода CVV2/CVC2 и т.д.).

ПРОСИМ ВАС НЕЗАМЕДЛИТЕЛЬНО ОБРАЩАТЬСЯ В БАНК ПРИ ВОЗНИКНОВЕНИИ СЛЕДУЮЩИХ СИТУАЦИЙ:

1. На компьютере, используемом для работы в интернет-банке, обнаружено вредоносное ПО (вирусы, «трояны» и т.д.).
2. В «Журнале сеансов работы» обнаружены факты проникновения в систему посторонних лиц (вход в систему с нетипичного IP-адреса либо в нетипичное для Вас время).
3. В выписке обнаружены несанкционированные Вами расходные операции, либо Вы получили SMS или e-mail-уведомление об операции, которую не совершали.
4. Вы получили SMS или e-mail-уведомление об изменении адреса e-mail или номера мобильного телефона для отправки уведомлений, при этом изменения были совершены без Вашего ведома.

Рекомендации по выбору пароля

Не делайте простые и легкие пароли (111111,12345,abcdefg,qwerty и т.п.). Не выбирайте в качестве пароля дату рождения, номер телефона и другие данные, которые легко узнать. Пароль должен быть не короче 8-ми символов. В числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@ # $ & * % и т.п.). Пароли должны быть незапоминающимися. При выборе между Password и Jfhru195ki1@_) отдайте предпочтение второму. Любой пароль со смысловой нагрузкой небезопасен.

Не передавайте пароли третьим лицам и не записывайте пароли на носители ключевой информации (токены, flash-карты, смарт-карты).