Памятка по соблюдению мер информационной безопасности при работе с Банк-клиентом

В настоящее время увеличивается количество хищений денежных средств клиентов банков, использующих систему ДБО (дистанционное банковское обслуживание). Одними из основных причин этого являются вирусное заражение ПК с ДБО и несоблюдение сотрудниками клиента мер информационной безопасности по хранению паролей и ключей с ЭП.

Вирусные программы массово распространяются в сети Интернет через взломанные сайты, социальные сети и другие сетевые сервисы, электронную почту, свободно распространяемое ПО и пр. Через сайты российских и международных социальных сетей (odnoklassniki.ru, vkontakte.ru, facebook.com и т.д.) и через рекламно-баннерные сети распространяется наибольшее количество вредоносных программ. При этом новые модификации вирусов, сигнатуры которых еще не включены в антивирусные базы, успешно преодолевают антивирусное ПО.

В этих условиях только жесткая политика в отношении доступа в Интернет и постоянное соблюдение всех рекомендаций информационной безопасности, приведенных в Памятке, позволяет минимизировать риск мошеннических действий против Вас.

Рекомендации по информационной безопасности для клиентов ООО Банк «Саратов».

1. Для работы с системой Банк-клиент необходимо подготовленное рабочее место, которое рекомендуется использовать **только для работы с системой ДБО**, соответствующее следующим требованиям:
   - наличие современного антивирусного программного обеспечения, работающего в интерактивном режиме и использующего актуальные базы вредоносных кода (вирусов) и нежелательных программ;
   - рекомендуется наличие настроенного и работающего персонального межсетевого экрана, это поможет предотвратить несанкционированный доступ к компьютеру из сети Интернет или из локальной сети;
   - использование лицензионного и/или полученного из доверенных источников, регулярно обновляющегося, программного обеспечения, что обеспечивает защиту от программных «закладок» и ошибок программного обеспечения;
   - проведение регулярного полного сканирования рабочего места антивирусным программным обеспечением, что позволяет выявить ранее пропущенный вредоносный код;
   - рекомендуется организовать периодическую проверку контроля целостности установленной системы ДБО и системного ПО;
   - отключение режима автозапуска сменных носителей;
   - проведение регулярной установки обновлений программного обеспечения, по мере их выпуска производителем;
   - **отсутствие средств удаленного доступа** «TeamViewer», «rAdmin», «VNC» и т.п.; отсутствие удаленного доступа к файлам рабочего места с системой ДБО;
   - функционирование всех программных и аппаратных средств в штатном (нормальном) режиме;
   - использование парольной защиты для учетных записей, имеющих право регистрироваться на данном рабочем месте, с выполнением обязательных требований по сложности паролей (не использовать имена, даты рождения, и широко используемые клавиатурные комбинации т.к. «12345678», «qwertyui» и т.д.; использовать как минимум буквы, цифры и различные регистры; минимальная длинна пароля 8 символов);
   - регулярная смена паролей на учетных записях, имеющих право регистрироваться на рабочем месте с системой ДБО, не реже одного раза в месяц;
   - использование для повседневной работы пользователя с ограниченными, минимальными правами. Не работайте на компьютере с правами Администратора.

2. Не открывайте подозрительные и неизвестные файлы и ссылки на неизвестные сайты, даже если они получены с известного адреса; не посещайте сайты, предлагающие быстро и бесплатно скачать различные файлы или программы, поскольку даже вход на такой сайт может угрожать безопасности рабочего места.

3. Необходимо строго ограничивать доступ к компьютеру, с которого ведется работа с системой ДБО.

4. Предусмотреть меры, исключающие возможность несанкционированного не обнаруживаемого изменения аппаратной части компьютера с установленной системой ДБО (например, путем опечатывания системного блока и разъемов ПК)

5. Для обеспечения идентификации, аутентификации и авторизации клиентов, подтверждения подлинности и неизменности платежных документов в системе ДБО используется система криптографической защиты информации (СКЗИ) сертифицированная в соответствии с законодательством Российской Федерации. При работе с СКЗИ и электронной подписью необходимо соблюдать следующие требования:

   - Сохранять в тайне пароль к ключу электронной подписи и хранить сам носитель с ключом электронной подписи в надежном месте, исключающем несанкционированный доступ к нему;
   - Использовать в качестве места хранения носителя с ключом электронной подписи персональный сейф.
   - Запрещается:
     - снимать несанкционированные копии с носителей ключевой информации;
     - выводить ключ электронной подписи на дисплей (монитор) электронно-вычислительной машины (компьютеры) или принтер;
     - устанавливать носитель с ключевой информацией в считывающее устройство рабочего места, аппаратные и (или) программные средства которого функционируют в непредусмотренных (нештатных) режимах, а также на другие компьютеры;
     - записывать на носители ключевой информации постороннюю информацию;
     - передавать носитель с ключевой информацией другим лицам и разглашать пароль к ключу электронной подписи;
     - оставлять подключенным к компьютеру носитель ключа электронной подписи **дольше, чем это необходимо** для работы с системой ДБО.
   - Соблюдать предписания правил (согласованных с ФСБ) пользования криптобиблиотеками, поставляемых для работы с системой ДБО (Выдержка из правил предоставляется Банком вместе с дистрибутивом ДБО).
   - Производить замену ключей электронной подписи до истечения срока их действия. Кроме того, необходимо проводить замену ключей электронной подписи во всех случаях увольнения и смены лиц, имеющих доступ к системе

Банк-Клиент, в том числе IT-специалистов, а также руководителей с правом подписи доверенностей на получение ключей электронной подписи, и в случае подозрений на компрометацию ключа электронной подписи.

- При компрометации ключей электронной подписи прекратить все операции с использованием этого ключа и немедленно проинформировать о факте компрометации Банк. Организовать внеплановую смену ключей электронной подписи.

6. По требованию Банка необходимо подтверждать свои платежные поручения, присланные по системе ДБО.

7. Регулярно просматривать информацию в системе ДБО для контроля проведенных операций и получения электронных сообщений.

8. Не отвечайте на подозрительные письма/звонки с просьбой выслать закрытый ключ ЭП, пароль или другую конфиденциальную информацию. **Сотрудники Банка никогда** не попросят Вас сообщить им пароль или выслать закрытый ключ ЭП.

9. Если возникли подозрения, что доступ к компьютеру и USB-носителю с ключом электронной подписи могли получить неуполномоченные лица, либо обнаружено проведение несанкционированных платежей, требуется незамедлительно известить Банк о данных фактах и заблокировать ключи проверки электронной подписи. Проинформировав сотрудников Банка о подозрительных операциях, произвести отзыв платежей. Немедленное обращение в Банк значительно повышает вероятность того, что похищенные денежные средства удастся возвратить и предотвратить мошенничество. В случае несвоевременной реакции вероятность быстрого возврата похищенных денежных средств значительно снижается и может потребовать обращения в правоохранительные органы.

10. К рискам Клиента использования системы ДБО относятся:

- получение несанкционированного доступа посторонних лиц к управлению счетами Клиента;
- потеря денежных средств со счетов Клиента при несанкционированном доступе к счетам Клиента;
- доступ посторонних лиц к конфиденциальной информации Клиента в системе ДБО