Рекомендации клиентам АО «Банк «Агророс» по повышению уровня информационной безопасности при работе с Системой ДБО

В последнее время в средствах массовой информации участились упоминания о хищениях денежных средств с использованием систем дистанционного банковского обслуживания (Система ДБО). Основными причинами хищения являются вирусное заражение компьютера или мобильного устройства клиента, с которых осуществляется работа с системами ДБО, а также несоблюдение сотрудниками клиента - юридического лица или самим клиентом основных мер по обеспечению сохранности логинов/паролей, ключевых носителей.

Возможными рисками при использовании системы ДБО являются:

- получение злоумышленником несанкционированного доступа к управлению счетами Клиента для вывода денежных средств на свои счета;
- доступ посторонних лиц к конфиденциальной информации Клиента в Системе ДБО.

Для минимизации рисков при использовании Системы ДБО АО «Банк «Агророс» рекомендует Вам проводить регулярный аудит безопасности ваших компьютеров и мобильных устройств, с помощью которых Вы пользуетесь Системой ДБО, и на постоянной основе выполнять все рекомендации приведенные ниже.

Рекомендации по повышению уровня информационной безопасности:

1. При подключении к Системе ДБО рекомендуем выбирать Усиленную электронную подпись (УЭП).
2. При входе в Систему ДБО необходимо проверять установление шифрованного канала связи: наличие символов https:// в адресной строке браузера. Также обязательно в адресе указывается agroros.ru. В зависимости от канала связи и от устройства с которого Вы заходите в ДБО адрес может варьироваться, например: https://dbo.agroros.ru/dbo/ или https://dbo2.agroros.ru/dbo/ или https://dbo.agroros.ru/pda/. В любом случае, обязательно должны присутствовать https:// и agroros.ru.
3. Клиентам – физическим лицам рекомендуем установить подтверждение входа в систему ДБО одноразовым паролем (дополнительный параметр, по которому Система ДБО будет разрешать Вам вход- одноразовый код из SMS-сообщения или код из Google Authenticator). Для установки необходимо пройти: «Меню» - «Система»-«Настройка параметров»-«Подтверждение входа в систему ДБО».
4. Обращайте внимание на новости и рекомендации, размещаемые Банком в Системе ДБО при входе.
5. Необходимо проверять последние адреса (IP-адрес) и время работы по списку, который предоставляет Вам Система при входе. Убедитесь, что в списке нет подозрительных адресов и времени работы. В противном случае – необходимо незамедлительно сообщить о данном факте в Банк.
6. Никому не сообщайте свои логин, пароль, не храните их записанными в общедоступных местах. При подозрении на их компрометацию необходимо незамедлительно сообщить в Банк, заблокировать доступ к Системе ДБО, сверить остатки

по своим счетам, организовать внеплановую смену пароля, ключей УЭП (при наличии) и только после этого возобновить работу с Системой ДБО.

7. Кодовое слово должно быть известно только уполномоченным/доверенным лицам, имеющим право доступа к Системе ДБО. Помните, кодовое слово признается Банком подтверждением того, что физическое лицо, сообщившее кодовое слово, надлежащим образом уполномочено Клиентом на получение информации, составляющей банковскую тайну такого Клиента.

8. Используйте надежные пароли как для доступа к Системе ДБО, так и для входа в компьютер:

- длина пароля не менее 8 символов (рекомендуется 12);
- пароль содержит буквы разных регистров (заглавные и строчные), цифры, символы;

Не используйте тривиальные пароли (свои ФИО, даты рождения детей, близких родственников, имена домашних питомцев, стандартные пароли «qwerty», «123456789», и т.п.).

Меняйте пароли не реже 1 раза в 90 дней, и немедленно - в случае подозрения на компрометацию пароля.

Не используйте одинаковые пароли для входа в Систему ДБО и доступа к социальным сетям, электронной почте и т.д.

9. Регулярно следите за состоянием Ваших счетов, операциями по счетам, статусами документов в Системе ДБО.

10. После проставления подписи в Системе ДБО необходимо проверять реквизиты подписанных документов (один из самых распространенных способов мошенничества – это замена реквизитов платежных документов в различных системах ДБО в момент подписания легитимным пользователем). Подключите услугу SMS-информирование, не оставляйте приходящие из Банка SMS без внимания (сверяйте реквизиты операции).

11. Никому не сообщайте одноразовые коды подтверждения из SMS-сообщений (если это не требуется в самом сообщении).

12. Для максимальной безопасности приобретите и используйте специально для ДБО самый простой телефон (без функции подключения к сети «Интернет», только с функциями звонка и SMS).

13. Следите за содержанием своего «белого списка» (список доверенных получателей платежей).

14. Предоставляйте в Банк документы, подтверждающие продление полномочий уполномоченных лиц до окончания срока их действия, а также незамедлительно сообщайте об отзыве таких полномочий.

15. Требования к компьютеру с которого осуществляется работа с Системой ДБО:

- используйте компьютер, с которого осуществляется работа с Системой ДБО только для работы с Банком и бухгалтерского учета. Не используйте данный компьютер для общения в социальных сетях. Не переходите по сомнительным ссылкам рекламы и новостей. В случае необходимости работы в сети Интернет используйте только проверенные сайты по заранее определенному списку адресов;

- используйте только лицензионное программное обеспечение (далее – ПО). Своевременно обновляйте операционную систему.
- используйте лицензионное антивирусное ПО с автоматическим обновлением. Проводите регулярное полное сканирование компьютера средствами антивирусного ПО;
- отключите автозапуск сменных носителей. Проводите сканирование сменных носителей антивирусным ПО при каждом подключении к компьютеру;
- ограничьте доступ посторонних лиц к компьютеру. Предусмотрите меры, исключающие возможность несанкционированного не обнаруживаемого изменения аппаратной части компьютера (например, путем опечатывания системного блока и неиспользуемых разъемов компьютера);
- не устанавливайте на компьютер непроверенные (без крайней необходимости – никакие) системы удаленного управления;
- не устанавливайте надстройки и плагины (например от поисковых служб Яндекс, Google и т.п., дополнительные панели, различные «интернет ускорители» и прочее) в программу интернет-браузер, которая используется для доступа к Системе ДБО;
- используйте для повседневной работы пользователя с ограниченными, минимальными правами. Не работайте с правами «Администратор»;
- используйте межсетевые экраны (персональный непосредственно на компьютере и/или в корпоративной сети), это поможет предотвратить несанкционированный доступ к компьютеру из сети Интернет или из локальной сети;
- при наличии технической возможности указывайте в заявке на подключение к Системе ДБО статический IP-адрес своего компьютера, с которого будет разрешен доступ к Системе.

16. Соблюдайте правила работы с электронной почтой: не открывайте вложения от неизвестных отправителей, не переходите по ссылкам полученным из недостоверных источников, не устанавливайте присланное ПО, если не уверены, что оно получено от доверенного источника. Если у Вас возникают сомнения, лучше свяжитесь с отправителем и уточните, что это точно он нам направил Вам сообщение – помните, Ваших знакомых, партнеров, контрагентов тоже могли взломать.

17. Ознакомьте своих сотрудников, уполномоченных/доверенных лиц, имеющих право доступа к Системе ДБО, с данными рекомендациями, контролируйте исполнение ими данных рекомендаций.

18. При увольнении уполномоченных лиц и иных сотрудников, имеющих доступ к Системе ДБО и/или к устройству с которого, осуществлялась работа с ДБО необходимо провести смену всех паролей к которым эти сотрудники имели (могли иметь) доступ, организовать смену кодового слова, провести полную антивирусную проверку рабочего места.

19. При использовании носителей ключей УЭП необходимо выполнять следующие правила:

- подключайте носитель ключей УЭП к компьютеру только на время работы с Системой ДБО;
- ни в коем случае никому не передавайте носитель;
- храните носитель в недоступном для посторонних лиц месте;

- при утере носителя или подозрении, что им могли воспользоваться без Вашего ведома необходимо незамедлительно сообщить о данном факте в Банк, заблокировать действующий сертификат подписи, сверить остатки по своим счетам и организовать внеплановую смену ключей УЭП.

20. При использовании мобильного устройства для работы с Системой ДБО и получения SMS-сообщений с одноразовыми кодами подтверждений:

- не оставляйте свой телефон (мобильное устройство) без присмотра;
- используйте 2 устройства: одно непосредственно для работы в Системе ДБО, второе (самый простой телефон только с функциями звонка и SMS) для получения SMS-сообщений с одноразовыми кодами подтверждений операций и входа в Систему;
- не пользуйтесь сетями общего доступа для работы с Системой ДБО, такие как wi-fi в общедоступных местах (кафе, кинотеатрах, торговых центрах);
- не используйте телефоны, у которых изменены заводские настройки в части доступа к операционной системе (Jail Break, Root и т.п.) Данные процедуры отключают защитные механизмы заложенные производителем;
- устанавливайте приложения только из официальных репозиториев мобильных приложений;
- используйте антивирусные программы для мобильных устройств, регулярно проводите антивирусную проверку своего устройства.

21. При утере мобильного телефона (выхода из строя SIM-карты), с подключенной услугой Системы ДБО (номер на который приходят SMS-сообщения с одноразовыми кодами подтверждения) необходимо незамедлительно обратиться к оператору своей сотовой связи для блокировки номера и в Контактный Центр Банка по телефонам, указанным на официальном Сайте Банка www.agroros.ru для блокировки доступа к системе ДБО.

22. При смене номера мобильного телефона, а так же при замене SIM-карты (в том числе с сохранением абонентского номера) необходимо незамедлительно обратиться в Банк для отключения старого номера и подключения нового и подтверждения замены SIM-карты. Помните, что операторы сотовой связи могут передать номер телефона другому абоненту.

23. При запросе от сотрудника Банка необходимо подтвердить факт направления платежных документов. Обращаем Ваше внимание, что сотрудник Банка никогда не попросит Вас сообщить пароль к Системе ДБО, одноразовый код подтверждения. Если у Вас появились сомнения в том, что Вам позвонил именно сотрудник Банка, не сообщайте никакой информации, а перезвоните самостоятельно в Банк по телефонам указанным на официальном сайте Банка www.agroros.ru

24. Обращаем Ваше внимание, что в соответствии с законодательством Российской Федерации Банк **обязан** приостановить операцию по переводу денежных средств на срок до двух рабочих дней, если у Банка появились подозрения, что она совершена без согласия Клиента. После приостановки операции сотрудник Банка связывается с Клиентом для подтверждения легитимности операции. В связи с этим настоятельно рекомендуем Вам следить, чтобы Ваши контактные данные, предоставленные Банку были всегда актуальны и доступны для связи.

В случае обнаружения в Системе ДБО ошибочных операций, возможных угроз безопасности Системы ДБО, фактов/подозрений на совершение мошеннических операций необходимо:

- незамедлительно сообщить о данном факте в Банк, для осуществления своевременной блокировки платежа и/или возврата денежных средств. После сообщения в течение 2-х дней необходимо будет предоставить в Банк письменное заявление на отмену платежа, совершенного без согласия Клиента;

- провести блокировку доступа к Системе ДБО, организовать смену ключей в Системе ДБО;

- обратиться с соответствующим заявлением в правоохранительные органы. Для того, чтобы у правоохранительных органов осталась возможность проведения расследования компьютер, с которого осуществлялся доступ в Систему ДБО необходимо выключить (желательно просто отключением питания, а не штатными средствами). Ни в коем случае не переустанавливайте операционную систему и не проводите полную антивирусную проверку компьютера до проведения всех необходимых действий правоохранительными органами. Работу с Системой ДБО (после смены паролей и при необходимости ключей ЭП) необходимо производить с нового компьютера.

Банк выполняет требования информационной безопасности, предъявляемые к оператору по переводу денежных средств, но обеспечить полную безопасность и сохранность Ваших денег без соблюдения Вами собственной информационной безопасности не представляется возможным!!!

Банк рекомендует Вам повышать свой уровень компьютерной грамотности, в том числе путем прохождения компьютерных курсов на уровне "продвинутого пользователя" при необходимости.