ПУБЛИЧНОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО

«МУРМАНСКИЙ СОЦИАЛЬНЫЙ КОММЕРЧЕСКИЙ БАНК»

Уважаемые Клиенты! В целях минимизации рисков, связанных с осуществлением несанкционированных переводов денежных средств с использованием системы дистанционного банковского обслуживания (далее – ДБО) «Банк-Клиент», заботясь о Вашей безопасности, БАНК «МСКБ» (ПАО) разработал следующие рекомендации по реализации защитных мер при использовании системы ДБО «Банк-Клиент»:

1. Используйте лицензионную операционную систему на компьютере, применяемом для работы в системе ДБО «Банк-Клиент». В операционной системе обязательно должна быть включена функция автоматической загрузки и установки обновлений операционной системы и прикладного программного обеспечения. В связи с тем, что с 8 апреля 2014 г. компания Microsoft прекращает техническую поддержку операционной системы Windows XP и выпуск автоматических обновлений, которые повышают защиту компьютера с системой ДБО «Банк-Клиент», настоятельно рекомендуем осуществить переход на современную версию операционной системы.

2. На компьютере, используемом для обеспечения работы системы ДБО «Банк-Клиент», должно быть установлено и включено антивирусное программное обеспечение и персональный сетевой экран с постоянно обновляющимися в автоматическом режиме базами. Например,
   - Kaspersky http://www.kaspersky.ru
   - ESET NOD32 http://www.esetnod32.ru
   - Dr.Web http://www.drweb.com
   - avast! http://www.avast.ru
   - Avira http://www.avira.com

3. Все прикладное и системное программное обеспечение, установленное на компьютере с системой ДБО «Банк-Клиент», должно быть лицензионным и получено из доверенного источника. Избегайте установки на компьютер ненужного программного обеспечения.

4. Работа пользователя в операционной системе с системой ДБО «Банк-Клиент» должна происходить в режиме «обычного пользователя» (классификация в системе Microsoft Windows – USER).

5. Установите сложные пароли на доступ в операционную систему, BIOS и систему ДБО «Банк-Клиент». Рекомендуем применять следующую парольную политику:
   - Длина пароля должна быть не менее 8 символов, при мощности алфавита не менее 10.
   - В числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п .).
   - Пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии и т. д.), а также общепринятые сокращения (USER, ADMIN, ALEX и т. д.).
   - При смене пароля новое значение должно отличаться от предыдущего не менее, чем в 4-х позициях.
   - Периодичность смены пароля не должна превышать 6-ти месяцев.
   - Число неудачных попыток ввода пароля должно быть ограничено числом 10.
   - Не осуществлять ввод пароля под наблюдением посторонних лиц.
   - Никогда не оставлять пароль в записанном виде.
   - Никогда не сообщать пароль иным работникам или третьим лицам.
   - Не хранить пароль в электронных файлах.

6. Рекомендуем отключить возможность автозапуска программ со всех подключаемых и встроенных устройств хранения данных, сетевых и сменных носителей информации («Панель управления» – «Автозапуск»).

7. Настоятельно рекомендуем отключить функцию подключения к удаленному рабочему столу операционной системы (Свойства системы – вкладка «Удаленный доступ» – «Не разрешать подключения к этому компьютеру»), а также исключить установку на компьютере с системой ДБО «Банк-Клиент» программ удаленного администрирования (Radmin, TeamViewer, Ammyy Admin и т.д.).

8. **Подключайте носитель с электронной подписью только на время подписания электронных платёжных документов в системе ДБО «Банк-Клиент», а в иное время обеспечьте его размещение в надежном хранилище (сейфе). Не оставляйте ключевой носитель без контроля, никогда не передавайте его ни при каких обстоятельствах третьим лицам, не копируйте данные с ключевого носителя на жесткий диск компьютера.**

9. **Используйте специальный аппаратно-программный комплекс для защищенного хранения ключевой информации (USB eToken).**

10. **Используйте услугу sms-информирования о движении по счету.**

11. **Ежедневно контролируйте движение по счету, получая выписки по нему.**

12. **Установите лимит на сумму одного платежа.**

13. **В случае возможности установите ограничение на право работы с системой ДБО «Банк-Клиент» с определенных сетевых адресов (IP) и физических адресов (MAC).**

14. Используйте для осуществления платежей выделенный компьютер. Ограничьте к указанному компьютеру физический доступ, путем размещения его в отдельном помещении с ограниченным доступом.

15. Постарайтесь не допускать третьих лиц к компьютеру с системой ДБО «Банк-Клиент», особенно оказывающих услуги аутсорсинга в области информационных технологий без заключения договора.

16. При работе в сети Интернет будьте бдительны, устанавливайте дополнительные программы и приложения, только если вы доверяете их разработчику. Никогда не открывайте вложения в письмах, полученных по электронной почте, от неизвестных отправителей.

17. С целью защиты от фишинг-атак (поддельные веб-страницы) при доступе в систему дистанционного банковского облуживания с использованием веб-клиента («легкий» браузерный «банк-клиент») осуществляйте постоянный визуальный контроль за адресной строкой web-обозревателя (браузера) на соответствие веб-адресу банка – https://dbo.bank-mscb.ru или https://дбо.банк-мскб.рф, а также на отсутствие ошибок в сертификате безопасности веб-узла.

ПУБЛИЧНОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО
«МУРМАНСКИЙ СОЦИАЛЬНЫЙ КОММЕРЧЕСКИЙ БАНК»

ВНИМАНИЕ!!!

- В случае выхода из строя компьютера с системой ДБО (например, компьютер неожиданно перезагрузился и больше не загружается).
- В случае выявления вредоносного программного обеспечения.
- В случае потери ключевого носителя или подозрения в его компрометации.
- В случае выявления электронных платежных документов в системе ДБО, передача которых не осуществлялась.
- В случае поступления информации (sms-информирование, выписки по счетам) об операциях по счету, которые не осуществлялись.

Немедленно сообщите об этом
в службу технической поддержки Банка с 08.30 до 18.00 по телефону – **(8152) 230-914**, либо операционному работнику с 08.30 до 16.00 по телефону – **(8152) 230-373.**