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» (АО) разработал следующие рекомендации по реализации защитных мер при использовании системы ДБО «Банк-Клиент»:

- 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.
- На компьютере, используемом для работы в системые ДБО «Банк-Клиент», должно быть установлено и включено антивирусное программное обеспечение и персональный сетевой экран с постоянно обновляющимися в автоматическом режиме базами.
- 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.
- Работу пользователя в операционной системе с системой ДБО «Банк-Клиент» рекомендуется организовать в режиме «обычного пользователя» (классификация в системе Microsoft Windows – Пользователи).
- Установите сложные пароли на доступ в операционную систему, BIOS и систему ДБО «Банк-Клиент».
- Рекомендуем отключить возможность автозапуска программ со всех подключаемых и встроенных устройств хранения данных, сетевых и сменных носителей информации.
- 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.).
- Подключайте носитель с электронной подписью только на время работы 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.
- Используйте услугу sms-информирования о движении по счету.
- Ежедневно контролируйте движение по счету, получая выписки по нему.
- Установите лимит на сумму одного платежа.
- В случае возможности установите ограничение на право работы с системой ДБО «Банк-Клиент» с определенных сетевых адресов.
- Используйте для осуществления платежей выделенный компьютер. Ограничьте к указанному компьютеру физический доступ, путем размещения его в отдельном помещении с ограниченным доступом.
- Постарайтесь не допускать третьих лиц к компьютеру с системой ДБО «Банк-Клиент», особенно оказывающих услуги аутсорсинга в области информационных технологий без заключения договора.

- 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.
- 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 , https://ibank.bank-mscb.ru или https://дбо.банк-мскб.рф, а также на отсутствие ошибок в сертификате безопасности веб-узла.

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**.