Требования к Клиенту по обеспечению безопасности при работе в системе «Интернет Клиент-Банк».

Для снижения рисков несанкционированного использования средств Клиента при использовании системы «Интернет Клиент-Банк» (далее Система), Банк «Кузнецкий мост»АО (далее Банк) рекомендует выполнять следующие требования информационной безопасности:

1. Обязательно использовать и регулярно обновлять антивирусное программное обеспечение на компьютере, используемом для работы с Системой. Еженедельно выполнять антивирусные проверки компьютера.
2. На рабочем месте для работы в Системе следует использовать только лицензионное ПО, а также регулярно устанавливать обновления операционной системы.
3. Не использовать компьютер, предназначенный для работы в Системе, для развлечений и просмотра произвольных интернет-страниц (интернет-серфинга). Не устанавливать и не сохранять подозрительные файлы, полученные из ненадежных источников, полученные по электронной почте, через мессенджеры, скачанные с неизвестных web-сайтов.
4. Ограничить доступ посторонних лиц к компьютеру, используемому для работы с Системой.
5. Подключать средство защищенного хранения данных (токен) к компьютеру только на время работы с Системой, не оставлять его подключенным к компьютеру даже на короткое время без необходимости.
6. Токен хранить в месте, исключающем несанкционированный доступ (в сейфе, запираемом шкафу). Пароль (PIN-код) для токена хранить отдельно от токена и только в распечатанном виде.
7. Рекомендуется использовать вариант подключения к Системе с двумя подписями. При этом работу каждого Уполномоченного лица следует выполнять с отдельного компьютера.
8. Следует использовать фаерволл на границе сети предприятия или персональный фаерволл на компьютере предназначенном для работы в Системе. Рекомендуется подключить в Банке услугу IP-фильтрации, ограничив доступ к Системе только с ip-адресов организации.
9. В начале работы каждого сеанса в Системе необходимо убедиться в правильности адреса Банка (*https://ib.kmbank.ru*) и в корректности SSL-сертификата Банка (иконка “закрытый замок” в адресной строке браузера).
10. Необходимо ежедневно получать выписку по счетам и сверять данные о проведенных операциях. При обнаружении несанкционированных операций в Системе следует незамедлительно связаться с Банком по телефону или любым другим способом.
11. Запретить удаленный доступ к ресурсам компьютера, используемого для работы в Системе. Не создавать на компьютере общие файловые ресурсы и не устанавливать программы для доступа к удаленному рабочему столу. При обнаружении подозрительной активности на компьютере (например, самопроизвольное движение курсора) следует немедленно извлечь токен. При наличии возможности, авторизоваться в Системе с другого компьютера и убедиться в отсутствии несанкционированных операций.
12. Необходимо следить за SMS-уведомлениями о совершенных платежах. При обнаружении SMS сообщений для подтверждения платежных поручений, которые не были созданы Клиентом, необходимо незамедлительно связаться с Банком по телефону, даже если подтверждаемые платежные поручения отсутствуют в системе.
13. При утрате токена, компрометации ключа электронной подписи, увольнении уполномоченных лиц необходимо незамедлительно связаться с Банком по телефону или любым другим способом и направить в Банк уведомление о компрометации ключа электронной подписи.

Следует помнить, что:

- Банк никогда не осуществляет рассылку электронных писем с просьбой предоставить конфиденциальную информацию, а также содержащих компьютерные программы.
- Если Вы получили письмо от имени Банка, содержание которого вызывает подозрение, либо с Вами связались по телефону от имени Банка, с просьбой установить какое-либо программное обеспечение или сообщить какие-либо коды из SMS-сообщений, просьба связаться со службой поддержки Банка и уточнить ситуацию. Всегда используйте контактную информацию служб поддержки Банка, указанную в официальных источниках информации, и не используйте контактную информацию, указанную в письме или полученную в ходе телефонного разговора.

Телефон службы поддержки Банка: *+7 (495) 510-63-91*

E-mail службы поддержки Банка: *internetbank@kmbank.ru*

Часы работы службы поддержки Банка: *Пн - Чт: 9:00-18:00, Пт: 9:00-17:00*