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

Использование Системы сопряжено с наличием рисков несанкционированного использования средств Клиента злоумышленниками: внутренними, в том числе персоналом Клиента, и внешними, как правило, использующими для хищения средств заражение компьютеров вирусами. С помощью электронных писем, при просмотре интернет страниц или после подключения инфицированного USB-накопителя (флеш карта, смартфон, внешний жесткий диск) компьютер Клиента может быть заражен вирусом. Далее злоумышленник скрытно устанавливает программное обеспечение для перехвата пароля на вход в систему и PIN кода доступа к устройству eToken, затем удаленно подключается к компьютеру Клиента и либо ждет удобного момента (когда подключено средство защищенного хранения данных eToken и компьютер оставлен без присмотра), чтобы скрытно создать и подписать электронной подписью платежное поручение от его имени, либо устанавливает дополнительное программное обеспечение для подмены реквизитов в платежных поручениях в момент создания для них электронной подписи.

Чтобы минимизировать риски Клиенту следует исполнять требования по обеспечению безопасности. Данные требования разработаны как для технических специалистов Клиента, так и для Уполномоченных лиц, непосредственно работающих в системе.

1. Обязательно следует использовать и регулярно обновлять антивирусное программное обеспечение. Наличие антивируса даже с актуальными базами в настоящее время не может полностью гарантировать того, что компьютер не будет заражен вирусом, однако значительно снижает данный риск.

2. Следует использовать межсетевой экран (фаерволл) либо на границе сети предприятия, либо персональный фаерволл на компьютере предназначенном для работы в Системе. Рекомендуется изолировать используемые в системе компьютеры от остальной сети предприятия, оставив открытыми только необходимые для работы порты. Рекомендуется разрешить подключение компьютера к серверу системы (https://ib.kmabnk.ru) и серверам обновлений используемого программного обеспечения, любые иные подключения рекомендуется запретить.

3. Не реже чем раз в неделю следует выполнять антивирусные проверки компьютера.

4. Подключить услугу IP-фильтрации, ограничив доступ к Системе только с ip-адресов организации.

5. Необходимо ежедневно получать выписку по счетам и сверять данные о проведенных операциях

6. Необходимо следить за SMS-уведомлениями о совершенных платежах. Быстро обнаруженное несанкционированное Клиентом платежное поручение, позволяет отозвать или приостановить его исполнение до того момента когда похищенные средства будут обналичены злоумышленниками.

7. 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.

8. Злоумышленники могут создать мошеннический ресурс с похожим на сайт Системы адресом и визуально похожим интерфейсом. Чтобы избежать ввода конфиденциальной информации на таком ресурсе, в начале работы каждого сеанса в Системе необходимо убедиться в правильности адреса Банка (https://ib.kmbank.ru) и в корректности SSL-сертификата Банка (Наличие иконки “закрытый замок” в адресной строке браузера).

9. На рабочем месте для работы в Системе следует использовать только лицензионное ПО, регулярно (не реже 1 раза в месяц) устанавливать обновления операционной системы (желательно в автоматическом режиме).

10. 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.

11. Не устанавливать и не сохранять подозрительные файлы, полученные из ненадежных источников, полученные по электронной почте, через службы мгновенного обмена сообщениями (ICQ, mail-агент), скачанные с неизвестных web-сайтов.

12. При завершении работы в Системе и при длительных перерывах извлекать средство защищенного хранения данных eToken из компьютера, не оставлять его подключенным к компьютеру

даже на короткое время без необходимости. Следует хранить средство защищенного хранения данных eToken в месте, исключающем несанкционированный доступ (в сейфе, запираемом шкафу).

13. Ограничить доступ к компьютеру посторонних лиц.

14. В случае использования смартфона для получения SMS сообщений от Банка не рекомендуется производить на нем операцию jailbreak (для ОС IOS) или получать root права (для ОС Android).

15. В случае использования смартфона для получения SMS сообщений от Банка не рекомендуется устанавливать приложения полученные не из доверенных магазинов приложений (например App Store, Google Play Market).

16. Не следует работать в Системе с компьютеров, по отношению к которым отсутствует уверенность, что принимаются необходимые меры обеспечения безопасности.

17. При ежедневной работе на компьютере не использовать права администратора. Следует установить пароли для входа пользователя и администратора в операционной системе. Рекомендуется использовать встроенный в операционную систему механизм контроля учетных записей (UAC) для защиты от несанкционированных действий.

18. Не использовать компьютер, предназначенный для работы в Системе, для развлечений и просмотра произвольных интернет-страниц (интернет-серфинга).

19. Рекомендуется вариант подключения к Системе с двумя подписями, в этом случае работу каждого Уполномоченного лица следует выполнять с отдельного компьютера.

20. При обнаружении подозрительной активности на компьютере (например, самопроизвольное движение курсора) следует немедленно извлечь средство защищенного хранения данных eToken. Если есть возможность, необходимо авторизоваться в Системе с другого компьютера и убедиться в отсутствии несанкционированных операций.

21. При обнаружении несанкционированных операций в Системе следует незамедлительно связаться с Банком по телефону или любым другим способом. Оперативное обращение в Банк может предотвратить несанкционированное списание средств, либо приостановить его, снизив финансовые потери.

22. При утрате средства защищенного хранения данных eToken, 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.

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.

Напоминаем, что основными способами электронного взаимодействия Банка и Клиентов являются штатные возможности и информационные каналы, предоставляемые Системой. Любые электронные сообщения, отправленные с бесплатных почтовых служб Интернет (@mail.ru, @yandex.ru, @rambler.ru, @gmail.com, @yahoo.com и т.п.), не являются почтой, отправленной Банком.