Рекомендации для клиентов по информационной безопасности при работе с системой дистанционного банковского обслуживания «iBank2»

В целях повышения безопасности работы в системе дистанционного банковского обслуживания «iBank2» (далее - Система «iBank2») КМ «Профильный Банк» (АО) (далее - Банк) обращает Ваше внимание на необходимость соблюдения мер предосторожности, которые повысят уровень Вашей информационной и финансовой безопасности.

С целью минимизации рисков доступа третьих лиц к работе с Системой «iBank2», а также совершения операций, соответствующих признакам перевода денежных средств без добровольного согласия Клиента, Банк настоятельно рекомендует придерживаться приведенных ниже правил:

- Для хранения файлов с ключами электронной подписи (далее - Ключ ЭП) использовать специализированные ключевые носители (usb-токены). При этом владелец usb-токена должен хранить его в условиях, исключающих доступ к нему третьих лиц, например, личный сейф.
- Подключить услугу «SMS-подтверждения», позволяющую подтверждать платежные поручения с помощью кода подтверждения, который направляется в виде sms-сообщения на номер мобильного телефона Клиента/представителя клиента.
- Ограничить доступ к Системе «iBank2», указав список компьютеров (IP-адресов), с которых Клиент будет производить работу в Системе «iBank2». Данное ограничение позволяет быть уверенным в том, что информация, передаваемая в Банк, будет обработана только в случае совпадения IP-адреса передающего компьютера с IP-адресом Клиента, хранящимся в базе данных Банка.
- Не допускать использования простых паролей, например, 123456, qwerty, и т.д. для учетных записей, имеющих право входа в операционную систему. Осуществлять периодическое изменение паролей, рекомендуемая периодичность изменения паролей не реже 1 (одного) раза в месяц.
- Не передавать Ключи ЭП сотрудникам для проверки работы Системы «iBank2» и проверки настроек взаимодействия с Банком. При необходимости проведения такой проверки владелец Ключа ЭП должен лично подключить носитель к компьютеру, убедиться, что пароль доступа к Ключу вводится в интерфейс клиентского АРМа «iBank2», и ввести пароль, исключая умышленное наблюдение посторонними лицами.
- Не передавать Ключи ЭП замещающим сотрудникам (заместителям, временно исполняющим обязанности). Для таких сотрудников необходимо получить персональные Ключи ЭП.
- При увольнении сотрудника, имевшего доступ к Ключу ЭП, обязательно заблокировать его Ключ ЭП.
- В случае если работа в Системе «iBank2» продолжительна, отключать и извлекать usb-токен с Ключем ЭП, если они не используются для работы. Usb-токен с Ключем ЭП должны находиться в компьютере только в момент подписания документов, и извлекаться сразу после подписания.
- Выделить отдельный компьютер, который будет использоваться только для работы с Системой «iBank2» и не выполнять на этом компьютере никакие другие задачи.
- Ограничить доступ к компьютерам, используемым для работы с Системой «iBank2» и исключить к ним доступ персонала, не работающего с Системой «iBank2».
- При обслуживании компьютера ИТ-сотрудниками, обеспечивать контроль над выполняемыми ими действиями.
- На компьютерах, используемых для работы с Системой «iBank2», исключить посещение интернет-сайтов сомнительного содержания. По возможности, полностью запретить все соединения с информационно - телекоммуникационной сети «Интернет» (далее -сеть Интернет), разрешив только доступ к необходимым ресурсам.
- Использовать только лицензионное программное обеспечение, обеспечив автоматическое обновление системного и прикладного программного обеспечения.
- Применять на рабочем месте лицензионные средства антивирусной защиты, обеспечив возможность автоматического обновления антивирусных баз, а также еженедельную полную антивирусную проверку.

- Осуществлять антивирусную проверку любых файлов, загружаемых из сети Интернет, полученных по электронной почте или на внешних носителях (дискеты, флеш-накопители, CD/DVD и др.).
- Не допускать работу в операционной системе под учетной записью, имеющей права администратора. Необходимо использовать учетную запись с ограниченными правами в операционной системе, установленной на компьютере.
- Запрещать использование любых средств удаленного (дистанционного) доступа, которые обычно используется IT-специалистами для удаленной поддержки. Заблокировать возможность использования таких средств с помощью файрвола (программного и/или аппаратного).
- При возникновении подозрений на несанкционированное использование Ключей ЭП или наличие в компьютере вредоносных программ – обязательно обратиться в банк для блокировки ключей ЭП.
- Если Вы заметили проявление необычного поведения программного обеспечения Системы «iBank2» или какие-то изменения в интерфейсе программы – позвонить в Банк и выяснить, не связаны ли такие изменения с обновлением версии программного обеспечения. Если нет – обратиться в банк для блокировки ключей ЭП. Банк обращает внимание на то, что:

  ✓ не имеет доступа к Вашим Ключам ЭП и не может от Вашего имени сформировать корректную ЭП под электронным платежным поручением;

  ✓ не осуществляет рассылку электронных писем с просьбой прислать Ваш Ключ ЭП или пароль;

  ✓ Банк не рассылает по электронной почте программы для установки на Ваши компьютеры. В случае если Вы получили подобное письмо от имени Банка, содержащее программу для установки или запрос на предоставление Ключей ЭП/паролей, необходимо незамедлительно сообщить об этом в Банк.

  ✓ ответственность за конфиденциальность Ваших Ключей ЭП лежит на Вас, как единственных владельцах Ключей ЭП;

  ✓ если Вы сомневаетесь в конфиденциальности своих Ключей ЭП или есть подозрение в их компрометации (несанкционированном использовании), Вы должны незамедлительно заблокировать Ваши Ключи ЭП;

  ✓ изменение пароля доступа к Ключу ЭП не защищает Вас от использования злоумышленниками Вашего ключа ЭП если он ранее уже получил дистанционный доступ к Вашему компьютеру.

Для получения дополнительной информации по техническим вопросам Вы можете обратиться в Банк: +7 (495) 646-73-22.