Рекомендации

о мерах безопасного использования системы дистанционного банковского обслуживания «iBank 2»

клиентами АО КИБ «ЕВРОАЛЬЯНС»-юридическими лицами и индивидуальными предпринимателями

Уважаемые клиенты!

Настоящие рекомендации разработаны АО КИБ «ЕВРОАЛЬЯНС» (далее – Банк) в целях:

- предотвращения хищения денежных средств, находящихся на Ваших банковских счетах при осуществлении расчетов с использованием системы дистанционного банковского обслуживания (далее – ДБО),
- доведения до клиентов Банка информации о возможных рисках получения несанкционированного доступа к системам ДБО с целью осуществления переводов денежных средств лицами, не обладающими правом распоряжения этими средствами, и о рекомендуемых мерах по снижению рисков проведения злоумышленниками несанкционированных платежей.

При работе с системой ДБО «IBank 2» рекомендуем:

1. **Соблюдать ОБЩИЕ МЕРЫ БЕЗОПАСНОСТИ при работе с системой ДБО:**
   - Не работайте с системой ДБО через публичные сети (кафе, рестораны, магазины, иные общественные места).
   - Используйте только собственные специально выделенные электронные устройства (компьютер, ноутбук, планшет). Не используйте чужие электронные устройства.
   - Прежде чем ввести пароль в системе ДБО, убедитесь, что соединение установлено именно с сервером Банка, в адресной строке браузера должен отображаться адрес https://ibank.euroalliance.ru. Обратите внимание, что адрес начинается с httpS:// («s» означает secured — защищенный). Рядом с адресной строкой Вы можете нажать на значок «замок» и проверить информацию о безопасности соединения с данным сайтом.
   - Перед началом работы в системе «IBank 2» выполните проверку компьютера или другого электронного устройства, с которого осуществляется работа с системой ДБО, на наличие вредоносных программ. В случае их обнаружения, незамедлительно прекратите работу с компьютером, отсоедините «IBank 2 Key» от компьютера, сообщите в Банк о возможной компрометации ключа.
   - При возникновении малейших подозрений и странностей в работе системы, в случае любых изменений в привычных для Вас процессах установления соединения с системой ДБО, немедленно обратитесь в службу технической поддержки Банка по телефону: **(4932) 59-01-01, 41-25-79, 8-800-700-92-22**.
   - Регулярно контролируйте состояние своих счетов в системе ДБО и незамедлительно сообщайте обо всех подозрительных или несанкционированных Вами финансовых операциях работникам Банка по телефону **(4932) 47-15-25, 8-800-700-92-92.**

- При возникновении любых подозрений на компрометацию ключа электронной подписи или компрометацию электронного устройства, с которого осуществляется работа с системой ДБО (наличие вредоносных программ), незамедлительно заблокируйте Вашу учетную запись в системе ДБО, сгенерируйте новые ключи электронной подписи и зарегистрируйте их в Банке.
- В случае сбоев в работе компьютера или иного устройства, с которого осуществляется работа с системой ДБО, его поломки во время сеанса работы с системой ДБО, или сразу после завершения сеанса работы (проблемы с операционной системой, жестким диском и т.п.), незамедлительно обратитесь в Банк по телефону **(4932) 47-15-25, 8-800-700-92-92** и убедитесь, что от Вашего имени не производились несанкционированные списания денежных средств с Ваших банковских счетов.
- В случае если у Вас неожиданно перестала работать СИМ-карта телефона, оперативно обратитесь к своему оператору сотовой связи для блокировки абонентского номера и замены СИМ-карты, а также обратитесь в Банк для выявления возможных несанкционированных операций.
- При потере телефона/смене номера телефона, а также в случае увольнения сотрудника, номер телефона которого использовался при работе с Банк-Клиент, обязательно обратитесь в Банк и произведите смену телефонного номера для получения sms-сообщений.

2. Обеспечить БЕЗОПАСНОСТЬ ЭЛЕКТРОННОГО УСТРОЙСТВА, которое используется для работы с ДБО (компьютер, ноутбук, планшет):

- Используйте для работы в системе ДБО специально выделенное для этих целей устройство (компьютер, ноутбук, планшет).
- Применяйте на Ваших электронных устройствах только лицензионное системное, прикладное и антивирусное программное обеспечение (далее – ПО).
- Своевременно устанавливайте обновления программного обеспечения, выпускаемого его производителями. Особенно обращаем внимание на необходимость использования актуальной версии среды исполнения Java, в которой работает «iBank 2».
- Используйте актуальную версию антивирусной программы. Своевременно, желательно в автоматическом режиме, устанавливайте обновления всех компонентов и информационных баз антивирусной программы.
- Еженедельно осуществляйте полную проверку электронного устройства, с которого осуществляется работа с системой ДБО, на наличие/отсутствие вредоносного кода.
- Установите на Вашем компьютере или другом электронном устройстве, с которого осуществляется работа с системой ДБО, специализированные средства безопасности – персональные межсетевые экраны (firewall), а также средние или высокие параметры безопасности и конфиденциальности установленного Интернет-браузера.
- Включите систему фильтрации ложных web-узлов (антифишинг) в своем Интернет-браузере, если Интернет-браузер её не имеет – обновите браузер.
- При работе в сети Интернет никогда не соглашайтесь на установку каких-либо дополнительных программ или компонентов, если Вы не уверены в их предназначении.

- Не открывайте письма и вложенные в них файлы, полученные по электронной почте от неизвестных Вам отправителей. Не переходите по ссылкам, содержащимся в подобных письмах. Открывайте файлы или интернет-ссылки, пришедшие по электронной почте даже от знакомых Вам людей только если они присланы Вам по Вашей просьбе. Помните, что сообщение может быть отправлено от имени Вашего знакомого человека вредоносной программой, захватившей контроль над его компьютером или учетной записью в социальной сети.
- Исключите посещение непроверенных Интернет-сайтов. Посещайте только сайты банков, с которыми работаете в рамках систем интернет-банкинга, и сайтов, где размещаются обновления систем безопасности разработчиков системного, прикладного и антивирусного ПО для данного устройства.
- В случае появления предупреждений Интернет-браузера о перенаправлении Вас на другой сайт при подключении к системе ДБО, немедленной обратитесь в **службу технической поддержки Банка по телефону: (4932) 59-01-01, 41-25-79, 8-800-700-92-22.**

3. ИСКЛЮЧИТЬ ДОСТУП ПОСТОРОННИХ ЛИЦ К ЭЛЕКТРОННОМУ УСТРОЙСТВУ, с которого осуществляется работа с системой ДБО:

- Назначьте ответственное лицо/ответственные лица, которые имеют право использовать систему ДБО.
- При смене ответственных лиц, которые имеют право использовать систему ДБО, а также при обнаружении или подозрении на доступ неуполномоченных лиц к ключевой информации в обязательном порядке произведите перегенерацию ключей и смену пароля.
- Определите порядок доступа и работы на электронном устройстве, с которого осуществляется работа с системой ДБО, исключающий доступ третьих лиц. Помните, что посторонние люди могут, в т.ч. преднамеренно, занести на компьютер вредоносные программы со своих носителей информации и/или путем посещения вредоносных сайтов в Интернет.
- Не доверяйте установку и настройку аппаратного и программного обеспечения временным IT-специалистам (например, по разовому договору, объявлениям в сети Интернет).
- Не предоставляйте приходящим администраторам и другим лицам возможность удаленного доступа к устройству, на котором работает система ДБО.
- Не устанавливайте на электронное устройство, с которого осуществляется работа с системой ДБО, программы он-лайн общения (ICQ, QIP, Skype и т.д.).
- Работайте на компьютере или другом электронном устройстве, на котором установлена система ДБО, только с правами пользователя (не администратора). Не отключайте UAC (user account control, контроль учетных записей пользователей) в системе Windows. Невыполнение этих требований существенно увеличивает риск заражения вредоносными программами. Учетная запись «Гость» на электронном устройстве, с которого осуществляется работа с системой ДБО, должна быть выключена.

4. ЗАЩИТИТЬ ПАРОЛЬ ДОСТУПА К КЛЮЧУ И КЛЮЧ ЭЛЕКТРОННОЙ ПОДПИСИ от хищения и копирования:

- Запомните пароль доступа к ключу электронной подписи. Никогда не записывайте его в местах, доступных посторонним лицам.

- Периодически (не реже одного раза в месяц) меняйте пароль доступа к ключу электронной подписи.
- Никому не сообщайте сведения о пароле, в т.ч. сотрудникам Банка. Помните, что Банк никогда не запрашивает эту информацию.
- Пароль доступа к электронной подписи не должен быть простым, должен содержать не менее 8 символов, включающие строчные и прописные буквы латинского алфавита, цифры, символы верхнего и нижнего регистра клавиатуры компьютера.
- Используйте для хранения ключей электронной подписи только специализированные устройства хранения «iBank 2 Key» – USB-токен, смарт-карту или трастскрин.
- В случае использования более одной электронной подписи, рекомендуем хранить подписи на разных устройствах «iBank 2 Key» и использовать их на разных компьютерах.
- Определите порядок доступа и места хранения ключей электронной подписи, мобильного телефона (сейф, запираемый шкаф), исключающие их несанкционированное использование неуполномоченными лицами.
- При увольнении ответственного работника, имевшего доступ к ключу электронной подписи, незамедлительно обратитесь в Банк с просьбой о блокировке Вашей учетной записи в системе ДБО, сгенерируйте новые ключи электронной подписи и зарегистрируйте их в Банке.
- Никогда не передавайте ключи IT-специалистам для проверки работы системы ДБО, проверки настроек связи с Банком и т.п. При осуществлении таких процедур ответственный за работу с системой ДБО должен самостоятельно подключить носитель электронной подписи и лично ввести пароль доступа к ключу, исключив возможность его просмотра третьими лицами.
- Отключайте и извлекайте носители ключей электронной подписи в то время, когда они не используются для работы в системе ДБО.
- Для подтверждения расчетных (платежных) документов всегда используйте sms-код.