Рекомендации по безопасности при работе с системой

«Банк-Клиент»

1. **При работе в Системе дистанционного банковского обслуживания «Банк-Клиент» (далее-Система БК):**

1.1. **Обеспечьте безопасность компьютера, с использованием которого осуществляется работа в Системе БК:**

1.1.1. Перед входом в Систему БК необходимо удостовериться в том, что на компьютере, с использованием которого осуществляется работа в Системе БК, отсутствует вредоносное программное обеспечение, на компьютере установлено, активировано и работает современное лицензионное антивирусное программное обеспечение, регулярно обновляются его антивирусные базы. Только регулярные обновление антивирусных баз и проведение антивирусных проверок позволит Вам своевременно обнаружить и предотвратить появление вредоносных программ (особенно важно контролировать обновление, если нет постоянного подключения к Интернету).

1.1.2. На компьютере рекомендуется использовать только лицензионное программное обеспечение, регулярно устанавливать рекомендуемые производителями обновления, как операционной системы, так и прикладного программного обеспечения, в том числе браузера, это позволит устранить выявленные уязвимости.

1.1.3. Рекомендуется использовать на вашем компьютере персональный межсетевой экран для входа в Интернет. Это позволит значительно снизить риск удаленного управления злоумышленниками из Интернет и локальной сети вашим компьютером и кражи вашей конфиденциальной информации. Дополнительно в настройках персонального межсетевого экрана рекомендуется разрешить подключение вашего Компьютера только к сайту Банка (https://ibam.ru), серверу Системы БК (https://ibam24.ru) и серверам обновлений разработчиков используемого программного обеспечения, любые иные подключения рекомендуется запретить.

1.1.4. Рекомендуется осуществлять работу в Системе БК с использованием отдельной учетной записи в операционной системе компьютера, защищенной сложным паролем, известным только Вам. При возможности рекомендуется осуществлять доступ в Систему БК с выделенного компьютера, используемого исключительно для работы с Системой БК. Права пользователя в операционной системе компьютера должны быть минимально необходимыми, должна быть запрещена установка прикладного программного обеспечения за исключением необходимого для работы в Системе БК.

1.1.5. Рекомендуется избегать работы в Системе БК с «недоверенных» компьютеров (в Интернет-кафе или другие общедоступные компьютеры, а так же «чужие» компьютеры временно используемые вами и т.п.). Крайне не желательно использование для работы в Системе БК публичных беспроводных сетей (например, бесплатный Wi-Fi и т.п.), вместо этого лучше воспользуйтесь «мобильным Интернетом» (GPRS / EDGE / HSPA / 3G / 4G соединение). В вышеописанных случаях существенно повышается риск кражи ваших конфиденциальных данных и денежных средств. Если же данные рекомендации Вами не выполнены, то сразу же при первой возможности измените пароль, войдя в Систему БК с «доверенного» Компьютера.

1.1.6. Не оставляйте без присмотра компьютер с активной Системой БК.

1.1.7. По возможности исключите посещение с данного компьютера сайтов сомнительного содержания и любых других потенциально опасных Интернет-ресурсов (социальные сети, форумы, чаты, телефонные сервисы и т.д.), а также чтение почты и открытие почтовых документов полученных из недостоверных источников.

1.2. **Выполняйте правила безопасности при работе в Системе Банк-Клиент**

1.2.1. Перед вводом логина и пароля при входе в Систему БК убедитесь, что соединение установлено именно со стартовой страницей Системы БК и в адресной строке web-браузера отображается https://ibam24.ru. Злоумышленники могут создать мошеннический ресурс с похожим адресом и визуально похожим на сайт Системы БК. Если вы заметили, что адрес сайта отличается или есть иные причины вызывающие подозрения в подлинности сайта (например, сообщение web-браузера о перенаправлении на другой сайт), то не вводите никакой конфиденциальной информации и незамедлительно сообщите о данном факте в Банк по телефону техподдержки (8 495-025-25-25 (доб.4). Рекомендуется вводить адрес Системы БК только вручную в адресной строке web-браузера и не переходить на данную страницу по ссылкам с Интернет ресурсов (за исключением https://www.ibam.ru/) или из сообщений по e-mail / в социальных сетях / СМС сообщений, даже если они отправлены от имени Банка.

1.2.2. При работе с Системой БК для обеспечения конфиденциальности весь трафик между Банком и вашим компьютером шифруется с помощью защищенного протокола TLS (Transport Layer Security). Перед началом работы в Системе БК необходимо удостовериться, что соединение установлено в защищенном режиме TLS. В префиксе в адресной строке web-браузера должен появиться символ S -https://ibam24.ru, а также отобразиться иконка «закрытый замок». Расположение иконки зависит от версии web-браузера, но как правило «закрытый замок» располагается в конце правой части адресной строки, либо в правом нижнем углу экрана. При клике на данное изображение должны отображаться сведения о сертификате (в строке сертификата «кем выдан» должно быть указано Thawte SSL CA), важно проверить наличие данных сведений так как мошеннические сайты могут содержать имитацию иконки «закрытый замок».

1.2.3. После окончания работы в Системе БК обязательно завершайте сеанс работы.

1.3. **Соблюдайте правила безопасности при работе с ключевыми носителями:**

1.3.1. Уделите вопросу хранения ключей Системы БК должное внимание. Помните, что наличие ключа позволяет заверить от Вашего имени документ и передать его на исполнение в Банк. Для большей безопасности храните ключи на съемных защищенных ключевых носителях (eToken, Рутокен).

1.3.2. Подключайте ключевой носитель к компьютеру только на время подписи документов. Не держите ключевые носители постоянно подключенными к компьютеру. Ни в коем случае не храните ключи на жестком диске компьютера.

1.3.3. Постарайтесь внедрить использование для отправки документов двух подписей (2-х ключей). Скомпрометировать два ключа сложнее, чем один.

1.3.4. При вводе ключа и пароля особое внимание обращайте на правильное отображение названия ключа.

1.3.5. При компрометации секретных ключей или компьютера, увольнения ответственного сотрудника или ИТ специалиста Вашей компании, который имел доступ к компьютеру или к секретным ключам незамедлительно сообщите в Банк для блокировки ключей и генерации новых.

1.4. **Соблюдайте правила безопасности при использовании паролей**

1.4.1. Для работы в Системе БК необходимо использовать только сложные пароли, удовлетворяющие следующим требованиям:

— пароль должен иметь длину от 8 до 20 символов, в нем должно быть не менее двух цифр и двух букв, допускается использование букв латинского алфавита, цифр, знаков ! # $ % & ( ) * + - . / : ; < = > ? [\ .

— пароль не должен содержать последовательности одинаковых символов и групп символов, легко угадываемые комбинации символов (dddddd, 333444555, qwerty, 12345, abc123 и т.п.)

— пароль не должен содержать связанных с Вами данных (имена и даты рождения членов семьи, адреса, телефоны, часть номера вашей банковской карты и т.п.)

— пароль не должен содержать словарных слов (passw0rd, football, shadow, sergey, natalia, русские слова, набранные в английской кодировке, например, Сергей – Cthutq).

— пароль не должен совпадать с предыдущими паролями и не должен совпадать с именем входа.

— пароль не должен быть копией или комбинаций паролей используемых Вами в других системах (операционная система компьютера, электронная почта, развлекательные ресурсы в Интернет и т.п.)

1.4.2. Никогда не сообщайте свой пароль третьим лицам, в том числе коллегам, родственникам и сотрудникам Банка, вводите пароль только при работе в Системе БК. Сотрудник Банка не имеет права запрашивать у Вас пароль, даже если вы самостоятельно обратились в Банк. Вводите пароль только в Системе БК, Банк никогда не отправляет сообщений с просьбой уточнить или предоставить пароль.

1.4.3. Не записывайте свой пароль там, где доступ к нему могут получить третьи лица. Запрещается сохранять пароль на компьютере, мобильном устройстве, а так же на иных электронных носителях, доступ к которым могут получить третьи лица.

1.4.4. Рекомендуется осуществлять смену пароля доступа к Системе БК не реже одного раза в 3 месяца.

1.4.5. При возникновении подозрений, что Ваш пароль стал известен третьим лицам, необходимо незамедлительно сменить пароль или заблокировать доступ в Систему БК, обратившись в Банк по телефону техподдержки (8 495-025-25-25 доб. 4).

В случае утраты, а также при возникновении любых подозрений, что Ваши логин и пароль стали известны третьим лицам (в том числе представившихся сотрудниками Банка) незамедлительно заблокируйте Вашу учетную запись в Системе БК. Вы можете сделать это, связавшись с Банком по телефону техподдержки (8 495-025-25-25 доб. 4).

1.5. **Остерегайтесь мошенничества:**

1.5.1. Банк никогда не связывается по телефону и не осуществляет рассылок сообщений по СМС или email с просьбой предоставить, подтвердить или уточнить Вашу конфиденциальную информацию (пароли, логины, кодовое слово, Ф.И.О., паспортные данные, номер мобильного телефона, который подключен к услуге SMS-информирования и другие конфиденциальные данные). Не отвечайте на такие сообщения.

1.5.2. Банк никогда не связывается с просьбой установить или обновить программное обеспечение, в своих электронных письмах никогда не рассылает программы. Не открывайте подозрительные файлы, присланные вам по электронной почте.

1.5.3. При получении подозрительного сообщения якобы от имени Банка не отвечайте на него, не переходите по ссылкам указанным в подозрительном сообщении (даже если адрес похож на адрес сайта Банка). В сообщениях Банка никогда не будет просьбы зайти в Систему БК по указанной в сообщении ссылке.

1.5.4. При работе с Системой БК обратите внимание на страницу входа и интерфейс, если вы заметите любые отличия, не заявленные ранее Банком, или возникнут иные причины для возникновения подозрений в том что сайт поддельный, необходимо незамедлительно прекратить работу и обратиться в Банк по телефону техподдержки (никогда не связывайтесь по телефону указанному на подозрительной странице).

1.5.5. Если вы самостоятельно связались с Банком, сотрудники могут уточнить у Вас персональную информацию, но не имеют права запрашивать у Вас пароль на вход в Систему БК.

1.5.6. Банк никогда не направляет сообщений о блокировке/разблокировке Вашей учетной записи в Системе БК. Сотрудники Банка никогда не связываются по телефону, чтобы сообщить о недоступности Системы БК вследствие проведения каких-либо регламентных работ. Если вы получили подозрительное сообщение от имени Банка, либо с Вами связались по телефону с одной из просьб, перечисленных в данном разделе, то рекомендуется сообщить о данном факте в Банк по телефону техподдержки (никогда не связывайтесь с Банком по телефону указанному в подозрительном сообщении).

1.5.7. Обращайте внимание на появление подозрительной активности на Вашем компьютере, например, самопроизвольные движение курсора на экране, набор текста и т.п. Обращайте внимание на невозможность зайти на сайт Системы БК, при том, что другие Интернет-сайты у Вас загружаются, а так же на невозможность войти в Систему БК по причине несовпадения логина и пароля, при том, что они корректны. Обращайте внимание на «зависания» Системы БК, при нормальной работе других Интернет сайтов. Данные факты могут свидетельствовать о заражении Вашего компьютера вредоносными программами. Избегайте работы в Системе БК с зараженных компьютеров, если на зараженном компьютере уже осуществлялась работа в Системе БК, то незамедлительно заблокируйте Вашу учетную запись. Вы можете сделать это, связавшись с Банком по телефону техподдержки (8 495-025-25-25 доб. 4).

1.5.8. В случае если, по Вашему мнению, произошло несанкционированное списание денежных средств, необходимо незамедлительно обратиться в Банк с сообщением о несанкционированном списании. В случае если операция не совершалась ни Клиентом, ни его Представителем, а так же имеются иные признаки незаконного завладения денежными средствами (кражи) с использованием Системы БК, то после обращения в Банк Вам рекомендуется оперативно обратиться с заявлением в правоохранительные органы о возбуждении уголовного дела по факту хищения денежных средств (глава 21 УК РФ). После чего предоставить в Банк копию заявления о возбуждении уголовного дела, либо копию талона-уведомления, подтверждающего непосредственное обращение в правоохранительные органы и содержащего порядковый номер из книги учета сообщений о преступлениях содержащую отметку правоохранительного органа о его приеме.

Помните, что Ваше оперативное обращение в Банк может предотвратить несанкционированное списание, либо приостановить списание денежных средств, снизив Ваши финансовые потери.