Уведомление о рисках, связанных с выполнением операций с использованием систем дистанционного банковского обслуживания (ДБО)

Данное Уведомление призвано ознакомить Клиента с рисками, связанными с осуществлением операций с использованием систем ДБО, ответственно подойти к вопросу об использовании систем ДБО и не имеет целью заставить Клиента отказаться от них.

Банк со своей стороны принимает все меры по защите информации.

Существуют следующие виды рисков (в компьютерах и сети Клиентов):

1. Риски возможного мошенничества (хищения средств со счета) при помощи подмены информации о проводимом платеже, при помощи создания неправомерного платежа и т.п.:
- с использованием вредоносных программ, уязвимых операционных систем;
- в результате получения удаленного доступа к компьютеру организации;
- с участием сотрудников Клиента;
- хищение средств приходящими по вызову нештатными специалистами, настраивающими программы или ремонтирующими компьютеры.
2. Риск технических сбоев – риск отказа в обслуживании по причине неработоспособности технических средств и линий связи. Следствие этого риска - несвоевременная отправка платежа.
3. Риск, связанный с передачей информации о финансовых операциях через каналы “SMS” и/или электронной почты – использование третьими лицами информации, к которой они получили доступ посредством неправомерного доступа к мобильному телефону или почтовому ящику, либо посредством перехвата сообщений.

Для минимизации вышеперечисленных рисков Клиенту необходимо соблюдать требования Соглашения о подключении к ДБО, а также выполнять следующие рекомендации:

При подключении к СДБО со стационарного компьютера, ноутбука:

- использовать на компьютере лицензионную операционную систему и настроить автоматическое ее обновление;
- использовать лицензионное антивирусное программное обеспечение с настроенным своевременным обновлением его;
- не передавать **неуполномоченным** лицам информацию пользователей системы дистанционного банковского обслуживания (учетные имена пользователей, электронные ключи, пароли, средств шифрования) и исключить иные возможности получения персональной информации пользователей системы дистанционного банковского обслуживания третьими лицами;
- использовать парольную защиту ключей электронной подписи (ЭП);
- подключать устройства, хранящие ЭП, только перед началом работы в системе ДБО и отключать сразу после окончания работы с ДБО;
- не оставлять без присмотра компьютер с активной сессией ДБО;
- не отвечать на подозрительные письма и запросы пришедшие по SMS или e-mail;
- своевременно сообщать в Банк о случаях компрометации ЭП или о подозрении на компрометацию ЭП;
- менять ЭП в случае увольнения сотрудника, имевшего доступ к ЭП;
- использовать услуги SMS-информирования о входе в систему ДБО и о проводимых по счетам операциях;
- Не завышать сумму платежного поручения, начиная с которой, требуется дополнительное подтверждение платежного поручения (сервис «Одноразовые пароли» для дополнительного подтверждения в СДБО «Клиент-Банк iBank2» и «Сервис дополнительного подтверждения» СДБО «Клиент+Банк»);
- внимательно сверять реквизиты платежных документов из СМС-сообщения с кодом подтверждения операции с реальными реквизитами получателя платежа;
- ***ежедневно*** просматривать выписки в системах ДБО, даже если Вы не проводили операции;
- работать на компьютере, где установлены системы ДБО ПАО «ЧЕЛИНДБАНК», только от имени учетной записи, не обладающей полномочиями администратора в ОС Windows;
- обязательно использовать пароль на вход в операционную систему. Этот пароль должен отвечать следующим требованиям сложности: длина пароля не менее 8 символов, пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, user и т.п.), пароль не должен совпадать с логином пользователя, при смене пароля новое значение не должно повторять одно из 4-х предыдущих значений пароля, пароль должен содержать не менее 2 неалфавитных символов (1,2,-,=, (@, #, $, &, *, % и т.п.), а также буквы в верхнем и нижнем регистре.
- производить смену паролей не реже одного раза в год в операционной системе и системе ДБО;
- ограничить доступ к компьютеру, где установлены системы ДБО, по сети. Включить и настроить брандмауэр Windows для предотвращения несанкционированного доступа к ресурсам компьютера или установить аналогичное ПО от других производителей. Следует отказаться от использования программ по удаленному управлению и администрированию (например: TeamViewer, radmin, VNC, remote desktop);
- при работе с системами ДБО внимательно вводить адрес страницы доступа к системе удаленного управления счетом. Очень часто мошенники регистрируют схожие с названиями банка доменные имена (Например, chellndbank.ru, chelindbahk.ru) и размещают на них собственные сайты, очень похожие по внешнему виду на сайты банков. Адреса страниц доступа к системе должен быть в точности соответствовать https://ibank.chelindbank.ru/, https://www.chelindbank.ru/ca. Точный адрес представительства нашего Банка в сети Интернет Вы всегда можете найти также на сайте Центрального Банка Российской Федерации (http://cbr.ru) в разделе «Информация по кредитным организациям»;

- обращать особое внимание на появление сообщений безопасности от Вашего Интернет-браузера при посещении указанных в предыдущем пункте страниц. Появление данных сообщений может свидетельствовать о том, что вас обманным путем перенаправили на мошеннический сайт, поэтому крайне нежелательно продолжать работу с данными страницами: вводить логины и пароли доступа к системе ДБО iBank2 либо, осуществлять процедуру генерации ключей СДБО «Клиент+Банк» либо производить другие действия, связанные с вводом логина, пароля либо Ваших персональных данных.

Рекомендации по мерам повышения информационной безопасности Вашей внутренней IT-инфраструктуры:

- использование статического IP-адреса для работы с системой ДБО (с одновременной привязкой логина к IP-адресу, работа с других IP-адресов будет запрещена);
- по возможности использовать специальный режим доступа к сети Интернет, желательно с выделением нескольких сегментов внутренней сети, различных по уровню доступа к Интернет, в том числе сегмента «демилитаризованной зоны». Только для компьютеров, находящихся в этой зоне, разрешены соединения по инициативе внешней сети (например, сайт предприятия размещается в сегменте «демилитаризованной зоны»), для всех других сегментов, соединения по инициативе внешней сети должны быть запрещены. Компьютеры с системами ДБО должны быть установлены в изолированном сегменте (в том числе и от локальной вычислительной сети предприятия), доступ в который из внешней и внутренней сети запрещен.

При подключении к СДБО с использованием мобильного приложения iBank2:

- Скачивать и устанавливать любые мобильные приложения, в том числе мобильное приложение iBank2, только из доверенных источников (Google Play, AppStore – для устройств, работающих под управлением Android и iOS соответственно);
- Не сохранять пароли для доступа к СДБО в мобильном приложении;
- Не передавать устройство с установленным приложением iBank2 третьим лицам. В случае кражи/утери мобильного устройства необходимо незамедлительно обратиться в Банк с заявлением о временной блокировке учетной записи для доступа к СДБО по телефону 8-800-5001-800;
- Использовать антивирусное ПО для мобильной платформы, соответствующей вашему устройству (Android/iOS);
- При установке на смартфон любых приложений обращать внимание на полномочия, которые они запрашивают. Не предоставлять разрешение на чтение контактов/СМС-сообщений тем приложениям, которым такой доступ не нужен для повседневной работы;
- Использовать последние версии операционной системы и мобильного приложения iBank2;
- Не использовать мобильное приложение на устройствах с модифицированной ОС, а именно устройствах Apple, прошедших через процедуру Jailbreak, либо Android-устройствах с активированным режимом «суперпользователя» (root);
- По возможности, настроить отправку СМС с кодами подтверждения либо уведомлениями об операциях по счету на другое мобильное устройство.

- **Всегда помните,** что дистанционное банковское обслуживание – это инструмент доступа к Вашему счету и денежным средствам, хранящимся на нем.
- **Банк не несет ответственности** за последствия несоблюдения Клиентом правил безопасности при работе с ДБО.
- **Клиент понимает** возможность появления данных рисков и согласен принять их на себя.
- **Клиент отказывается** от любых претензий к Банку за неполучение сообщения в случае повреждения/нарушения настроек электронной почты, отключения мобильного телефона, возникновения технической проблемы с телефоном, нахождения телефона вне зоны покрытия, а также при блокировке номера либо несвоевременном оповещении Банка о факте утери мобильного телефона или изменения номера.
- **Клиент уведомлен**, что Банк, ни при каких условиях не просит предоставлять какую-либо информацию о себе посредством SMS сообщений или сообщений по электронной почте.

Клиент:
Руководитель _____ _____ “___”_____ 20____ г.
Ф.И.О. *подпись*

МП

Уведомление о рисках до клиента доведено
Сотрудник Банка:

_____/_____/
(подпись) (ФИО)

«_____»_____ 20__ г.