Приложение
к Условиям обслуживания в Системе «Интернет-Банк»

ПРАВИЛА БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ СИСТЕМЫ «ИНТЕРНЕТ-БАНК»

Требования по соблюдению мер безопасности, содержащиеся в настоящих Правилах безопасности при использовании Системы «Интернет-Банк» (далее - Правила безопасности), являются обязательными и направлены на предотвращение возникновения финансовых потерь в результате совершения противоправных действий в отношении Клиента и его операций с использованием Системы «Интернет-Банк». В случае нарушений Клиентом Правил безопасности, например, при разглашении Логина, Пароля, персональных данных, Система «Интернет-Банк» (далее - Система) становится источником повышенного риска несанкционированного списания денежных средств со Счетов Клиента.

1. Клиент обязан хранить в секрете Логин, Пароль, Код доступа в Систему:

– не сообщать никому Логин, Пароль и Код доступа даже своим близким, работникам Банка (включая работников безопасности, технической поддержки и т.д.), сотрудникам правоохранительных органов и иным третьим лицам. Во время первого входа в Систему Клиенту необходимо сменить Первоначальный Пароль на постоянный Пароль, который создается Клиентом самостоятельно и используется при каждом входе в Систему. В качестве Пароля не следует использовать: ИНН; имена; фамилии; последовательности, состоящие из повторяющихся или одних цифр, в том числе номера телефонов, памятные даты, номера автомобилей и другую информацию, которую можно прямо или косвенно связать с Клиентом. Пароль должен содержать: большое количество символов (не менее 8 (восьми), буквенно-цифровую смесь, заглавные и строчные буквы, а также спецсимволы (например, `~!@#$%^&*()_-+={}[]\|:;”’<>,.?/);

– если Логин, Пароль и Код доступа стали известны постороннему лицу, их необходимо обязательно изменить сразу после получения Клиентом этой информации;

– запрещается хранить Логин, Пароль и Код доступа вместе с устройством, с использованием которого Клиент осуществляет доступ в Систему;

– запрещается сохранять Логин, Пароль, Код доступа в текстовых файлах на компьютере либо на других электронных носителях информации, так как это может привести к их краже и компрометации;

– запрещается записывать Логин, Пароль, Код доступа в память мобильного телефона без их шифрования или без установления соответствующей блокировки мобильного телефона. Несоблюдение данного правила может привести к тому, что в случае кражи/утери телефона, содержащего сведения о Логине, Пароле и Коде доступа мошенники получают полный доступ к денежным средствам Клиента;

– не предоставлять возможность совершения операций в Системе третьим лицам (в том числе своим близким) после самостоятельного входа в Систему;

– не использовать функцию автозаполнения в браузере, это позволит не сохранять конфиденциальную информацию о Логине и Пароле в памяти браузера, что предотвратит возможность ее использования посторонними лицами;

– для повышения степени защищенности Пароля от перехвата злоумышленниками использовать для ввода пароля имеющуюся в Системе виртуальную клавиатуру.

2. Клиент обязан использовать только официальные версии Системы «Интернет-Банк», Мобильного приложения Банка, размещенные на Сайте Банка, а также (при наличии технической возможности) в магазине приложений RuStore. Запрещается устанавливать Мобильное приложение по ссылкам из мессенджеров, sms-сообщений или электронных писем.

3. Запрещается предоставлять посторонним лицам сведения о своих персональных данных, Логин, Пароль, SMS-коды в ответах на электронные письма, sms-сообщения или звонки, в которых от имени Банка предлагается предоставить такие данные. В случае сомнений, что звонок или сообщение исходят из Банка, а также в случае подозрений, что в отношении Клиента совершается попытка мошеннических действий, следует самостоятельно перезвонить по телефону, указанному на Сайте Банка или на обратной стороне Карты Банка, в Единую службу поддержки клиентов:

8 800 1001111 (круглосуточно);

8 812 3358500 (круглосуточно);

+7 495 7211001(круглосуточно);

Клиенту необходимо всегда иметь при себе контактные телефоны Банка. До момента обращения в Банк Клиент несет риск, связанный с несанкционированным списанием денежных средств со Счетов.

4. Клиент обязан хранить в секрете SMS-коды на вход в Систему и на подтверждение Распоряжений в Системе, направляемые Банком на Номер мобильного телефона / в Мобильное приложение Клиента в целях дополнительной идентификации при входе в Систему и при совершении операций – это конфиденциальная информация, которую ни при каких обстоятельствах нельзя раскрывать никому, включая работников Банка и сотрудников правоохранительных органов. Работники Банка и сотрудники правоохранительных органов никогда не просят сообщить, выслать по электронной почте или ввести куда-либо, помимо Системы, конфиденциальную информацию (Пароль для доступа в Систему или SMS-коды, необходимые для осуществления операций в Системе).

5. В случае поступления sms-сообщения / Push-уведомления / рассылки по электронной почте / сообщения в социальных сетях / мессенджерах / Интернет-сервисах или звонка / личного обращения третьих лиц, в том числе представившихся работниками Банка (например, службы безопасности, службы технической поддержки и т.п.) или сотрудниками правоохранительных органов, побуждающих незамедлительно произвести действия в Системе (например, по разблокировке Карты, остановке выдачи кредита, отмене перевода денежных средств, перевода денежных средств на «безопасный» или «специальный» счет и т.п.) путем сообщения конфиденциальной информации (Логин, Пароль, Код доступа, SMS-код),

Клиенту запрещается:

– предоставлять запрашиваемую информацию;

– проводить любые действия/операции по инструкциям, полученным указанными способами;

– устанавливать приложения, программы удаленного доступа (AnyDesk, AirDroid, AirMore, TeamViewer и пр.) по инструкциям, полученным указанным способом;

– включать трансляцию экрана в мессенджерах по просьбе звонящих третьих лиц;

– предоставлять третьим лицам доступ к личному кабинету на сайте Федеральной государственной информационной системы «Единый портал государственных и муниципальных услуг (функций)» (www.gosuslugi.ru) в сети Интернет.

Клиенту следует незамедлительно:

– прервать общение с мошенниками (завершить телефонный разговор, не отвечать на sms-сообщения / Push-уведомления / e-mail-рассылку / сообщения в социальных сетях / мессенджерах / Интернет-сервисах);

– уведомить Банк о случившемся.

6. В целях информационного взаимодействия с Банком следует использовать только реквизиты средств связи (мобильных и стационарных телефонов, факсов, интерактивных Интернет-сайтов, обычной и электронной почты и пр.), указанных в документах, полученных непосредственно в Банке, либо размещенных на Сайте Банка.

7. При работе с Системой следует убедиться в отсутствии посторонних символов в адресной строке браузера. Для осуществления доступа в Систему используется адрес https://i2.abr.ru.

Мошенники создают поддельные сайты, дизайн и адрес которых очень похожи на оригинальные. На этих сайтах указывают номера телефонов, при звонках на которые пытаются ввести в заблуждение, завладеть информацией о персональных данных, Логине, Пароле, SMS-кодах, либо предлагают оставить (ввести) Пароль и Логин на поддельном сайте. В случае обнаружения такого сайта, следует обязательно сообщить об этом по телефону Единой службы поддержки клиентов.

8. Если на мобильный телефон Клиента пришло сообщение с SMS-кодом для подтверждения операции, которую Клиент не совершал, то существует вероятность, что устройство, с которого Клиент осуществляет доступ в Систему, заражено вирусом. Запрещается использовать этот SMS-код, даже если Клиенту позвонит человек, представится работником Банка и попросит сделать это. Следует немедленно сообщить в Банк о получении такого сообщения по телефону Единой службы поддержки клиентов, а также получить рекомендации о действиях по предотвращению мошенничества. Обновить антивирусные базы на этом устройстве и выполнить его полную проверку на вирусы, не использовать устройство для доступа в Систему до выполнения полученных рекомендаций и указанных выше действий.

9. При работе с Системой следует убедиться, что соединение с ней осуществляется в защищенном режиме. Признаком использования защищенного соединения является наличие справа или слева от адресной строки, либо справа вверху/внизу строки браузера изображения значка закрытого замка.

10. Клиенту рекомендуется устанавливать на мобильный телефон, на который Банк отправляет Пароли для доступа в Систему и SMS-коды, необходимые для осуществления операций в Системе, приложения, полученные только из известных источников. Банк высылает Пароли для доступа в Систему, SMS-коды для осуществления операций в Системе, а также информацию о параметрах исполнения операций с использованием Системы, только с номера с именем «ABR».

11. Клиенту не рекомендуется заходить в Систему с того же мобильного телефона, на который Клиент получает пароли для доступа в Систему и SMS-коды для осуществления операций в Системе.

12. Следует внимательно проверять поступающую на мобильный телефон Клиента информацию о параметрах исполнения операции с использованием Системы. Информация в сообщении должна совпадать с параметрами операции в Системе. Клиент обязан убедиться, что сумма и наименование получателя (точки обслуживания) в sms-сообщении/Push-уведомлении совпадают с суммой операции и наименованием получателя (точки обслуживания), в адрес которого осуществляется перевод. При наличии несовпадений следует немедленно обратиться по телефону в Единую службу поддержки клиентов.

13. Следует осуществлять переводы денежных средств по реквизитам, полученным только из известных источников. Не переводить денежные средства по реквизитам, полученным в sms-сообщениях/ сообщениях по электронной почте / сообщениях в социальных сетях/ мессенджерах / при звонке / личном общении от незнакомых лиц. В случаях поступления sms-сообщений/ сообщений по электронной почте / сообщений в социальных сетях / мессенджерах от родственников/знакомых/друзей с просьбой перевести денежные средства рекомендуется перед совершением операции по переводу денежных средств убедиться в личности отправителя сообщения (в том числе путем совершения звонка) в целях исключения мошеннических действий.

14. На устройствах, используемых для осуществления операций в Системе, в том числе для получения паролей доступа в Систему и SMS-кодов для осуществления операций в Системе (в том числе планшетах, смартфонах, компьютерах и пр.) следует установить средства антивирусной защиты, антивирусные базы которых должны обновляться не реже одного раза в сутки. Рекомендуется использовать дополнительные программы для

обеспечения безопасности этих устройств – межсетевые экраны, программы защиты от спам-рассылок и пр.

15. Мобильный телефон, используемый Клиентом для получения Паролей для доступа в Систему и SMS-кодов для осуществления операций в Системе, следует защитить паролем на вход и, если это возможно, на просмотр SMS-сообщений. Это не позволит посторонним лицам получить доступ к Паролям для работы в Системе в случае, если они получили доступ к мобильному телефону Клиента.

16. В случае утраты мобильного телефона, на который Банк отправляет Пароли для доступа в Систему или SMS-коды для осуществления операций в Системе, Клиенту следует незамедлительно обратиться к своему оператору мобильной связи и заблокировать телефонную SIM-карту.

17. В случае совершения в отношении Клиента противоправных действий со стороны третьих лиц Клиенту следует незамедлительно обратиться в полицию.