Вместе с РОССИЕЙ
БАНК РОССИЯ

Акционерное общество
«Акционерный Банк «РОССИЯ»

ПАМЯТКА
о мерах безопасного использования Системы «Интернет-Банк» для физических лиц

Работа с системой «Интернет-Банк» (далее – Система) осуществляется через общедоступную сеть Интернет, поэтому АО «АБ «РОССИЯ» (далее – Банк) предпринимает все необходимые организационные и технические меры, направленные на предотвращение несанкционированного доступа посторонних лиц к конфиденциальной информации, связанной с использованием Системы.
Вместе с тем, чтобы работа в Системе была удобной и максимально защищенной от мошеннических действий со стороны посторонних лиц, с Вашей стороны также требуется соблюдение следующих правил безопасной работы.

1. Обеспечивайте сохранность Вашего пароля для доступа в Систему:
   - не сообщайте никому свой пароль, даже своим близким и работникам Банка (включая работников безопасности, технической поддержки и т.д.). Пароль должен выбираться Вами самостоятельно, он не должен быть известен никому, кроме Вас;
   - 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 Вами;
   - если Ваш пароль стал известен постороннему лицу, его необходимо обязательно изменить сразу после получения Вами этой информации;
   - не следует хранить пароль вместе с устройством, с использованием которого Вы осуществляете доступ в Систему;
   - не сохраняйте Ваш пароль в текстовых файлах на компьютере либо на других электронных носителях информации, так как это может привести к его краже и компрометации;
   - не используйте функцию автозаполнения в Вашем 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 Вашего пароля от перехвата злоумышленниками используйте для ввода пароля имеющуюся в Системе виртуальную клавиатуру.
2. Корректно завершайте работу в Системе. Завершение работы выполняется путем выбора соответствующего пункта меню «Выйти из системы» – это удалит из браузера информацию о параметрах Вашей работы в Системе.
3. Пароль на подтверждение Вашего распоряжения в Системе – это Ваша конфиденциальная информация, которую ни при каких обстоятельствах нельзя раскрывать никому, включая работников Банка.

   Помните, что работники Банка никогда не просят сообщить, выслать по электронной почте или ввести куда-либо, помимо Системы, конфиденциальную информацию (пароль для доступа в Систему или цифровой код безопасности, необходимый для осуществления операций в Системе).

4. Защитите свой мобильный телефон. Устанавливайте на мобильный телефон, на который Банк отправляет пароли для доступа в Систему и цифровые коды безопасности, необходимые для осуществления операций в Системе приложения, полученные только из известных источников.
   Помните, что Банк высылает пароли для доступа в Систему, цифровые коды безопасности для осуществления операций в Системе, а также информацию о параметрах исполнения Ваших операций с использованием Системы, только с номера ABR.
5. Не рекомендуется заходить в Систему с того же мобильного телефона, на который Вы получаете пароли для доступа в Систему и цифровые коды безопасности для осуществления операций в Системе.
6. В случае утраты мобильного телефона, на который Банк отправляет пароли для доступа в Систему или цифровые коды безопасности для осуществления операций в Системе, Вам следует незамедлительно обратиться к своему оператору мобильной связи и заблокировать телефонную SIM-карту.
7. Если у Вас появились подозрения на то, что в отношении Вас совершается попытка мошеннических действий, незамедлительно обратитесь в единую круглосуточную службу поддержки Банка по телефону 8 800 5003322.
8. Используйте для телефонной связи с Банком только номер телефона единой круглосуточной службы поддержки 8 800 5003322. Мошенники могут указывать на поддельных сайтах номера телефонов, при звонках на которые Вас будут пытаться обмануть.
9. Если на Ваш мобильный телефон пришло сообщение с цифровым кодом безопасности для подтверждения операции, которую Вы не совершали, то существует вероятность, что устройство, с которого Вы осуществляете доступ в Систему, заражено вирусом. Не используйте этот одноразовый пароль, даже если Вам позвонит человек, представится работником Банка и попросит сделать это.

   Обязательно сообщите в Банк о получении Вами такого сообщения по телефону единой круглосуточной службы поддержки Банка 8 800 5003322, а также для получения рекомендаций о Ваших действиях по предотвращению мошенничества. Обновите антивирусные базы на этом устройстве и выполните его полную проверку на вирусы, не используйте устройство для доступа в Систему до выполнения полученных рекомендаций и указанных выше действий.
10. Внимательно проверяйте поступающую на Ваш мобильный телефон информацию о параметрах исполнения Вашей операции с использованием Системы. Информация в сообщении должна совпадать с параметрами Вашей операции в Системе. При наличии несовпадений следует немедленно обратиться в единую круглосуточную службу поддержки Банка по телефону 8 800 5003322.
11. На устройствах, используемых для осуществления операций в Системе, в том числе для получения паролей доступа в Систему и кодов безопасности для осуществления операций в Системе (в том числе планшетах, смартфонах, компьютерах и пр.) должны быть установлены средства антивирусной защиты, антивирусные базы которых должны обновляться не реже одного раза в сутки.

    Используйте дополнительные программы для обеспечения безопасности этих устройств – межсетевые экраны, программы защиты от спам-рассылок и пр.
12. Мобильный телефон, используемый для получения паролей для доступа в Систему и кодов безопасности для осуществления операций в Системе, следует защитить паролем на вход и, если это возможно, на просмотр SMS-сообщений. Это не позволит

посторонним получить доступ к Вашим паролям для работы в Системе в случае, если они получили доступ к Вашему телефону.

13. При работе с Системой убедитесь в отсутствии посторонних символов в адресной строке браузера. Для осуществления доступа в Систему используется адрес https://i.abr.ru.

    Вас могут пытаться обмануть, предлагая оставить Ваши пароль и логин на поддельном сайте. Если Вы обнаружите такой сайт, обязательно сообщите об этом по телефону единой службы круглосуточной поддержки клиентов 8 800 5003322.

14. При работе с Системой убедитесь, 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.

    Надеемся, что соблюдение этих несложных правил, которые значительно повышают безопасность использования системы «Интернет-Банк», не причинит Вам неудобств.