**ПАМЯТКА КЛИЕНТУ О РИСКАХ ПРИ ИСПОЛЬЗОВАНИИ
СИСТЕМ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ**

Уважаемые клиенты!

**ООО «Банк РСИ» информирует о возможных рисках при использовании систем дистанционного банковского обслуживания, связанных с попытками мошеннических действий.**

В настоящее время популярны следующие виды мошенничеств:

- направление поддельных электронных писем от имени официальных организаций, содержащих во вложении программное обеспечение с вредоносным кодом, или ссылку на программное обеспечение с вредоносным кодом. При скачивании и запуске такого вредоносного кода злоумышленник может получить возможность удаленного доступа в систему дистанционного банковского обслуживания;

- имитация злоумышленниками Интернет-представительств (web-сайтов) банков. Доменные имена и стиль оформления таких сайтов сходны с именами подлинных web-сайтов банков, при этом посетителям таких сайтов сообщают заведомо ложные банковские реквизиты и контактную информацию. При посещении таких поддельных сайтов злоумышленник может обманным путем получить данные для авторизации в системах дистанционного банковского обслуживания (при вводе информации в поддельные поля);

- направление злоумышленниками сообщения электронной почты якобы от имени технической поддержки банка. В сообщении под какими-либо предлогами (обновление программного обеспечения, проверка данных и т.п.) предлагают сообщить конфиденциальные данные. Также может быть дана ссылка для захода якобы в систему дистанционного банковского обслуживания. Мошенники могут указать, что другой адрес не доступен по причине технического сбоя. Пользователь может воспользоваться поддельной ссылкой, ввести свои данные для авторизации в системах дистанционного банковского обслуживания. После этого ему может быть выдано сообщение об ошибке, и он будет отправлен на сайт настоящей в системы дистанционного банковского обслуживания, где сможет увидеть всю необходимую ему информацию. Пользователь может даже не догадываться, что зайдя на подложный сайт, он уже передал свои данные злоумышленникам.

- попытки неправомерного получения персональной информации пользователей систем дистанционного банковского обслуживания (пароли, секретные ключи средств шифрования и аналогов собственноручной подписи, ПИН-коды и номера банковских карт, а также персональные данные их владельца). Попытки могут осуществляться путем направления поддельных ссылок, поддельных SMS сообщений на номера мобильных телефонов (могут содержать вида “ваша карта заблокирована”, “платеж на сумму зарегистрирован” и пр.).

**ООО «Банк РСИ» рекомендует меры по предотвращению несанкционированного доступа к системам дистанционного банковского обслуживания:**

1. При получении писем от официальных органов связаться с представителем организации по телефону и уточнить, направлялось ли письмо.
2. Обращать внимание на размещаемую в письме информацию (несовпадение написания адреса электронной почты и данных отправителя в подписи, стиль написания содержит ошибки, ссылки ведут на web-сайты, имеющие случайные символы в написании или не относящиеся к России домены (иные кроме RU домены в адресе)).
3. Использовать лицензионное средство антивирусной защиты, базы данных средства антивирусной защиты должны обновляться ежедневно; использовать дополнительные средства защиты от несанкционированного доступа (межсетевые экраны).
4. Не устанавливать приложения из не доверенных источников, от неизвестных разработчиков/издателей и т.п. лиц. По возможности минимизировать перечень установленного на рабочем месте программного обеспечения.
5. Контролировать написание адреса в строке браузера при доступе в систему дистанционного банковского обслуживания.
6. При получении писем с альтернативными ссылками системы дистанционного банковского обслуживания по официальному телефону Банка у сотрудника технической поддержки уточнять достоверность информации.
7. Не передавать персональную и конфиденциальную информацию (ПИН коды, логины, пароли) посторонним неуполномоченным лицам (в том числе представляющимися сотрудниками банков).
8. Игнорировать электронные сообщения с просьбой ввести конфиденциальную информацию на сайтах или отправить в письме электронной почты, так как уполномоченные сотрудники Банка не занимаются подобной рассылкой.
9. Игнорировать SMS и телефонные сообщения автоинформаторов, преследующих цель получение конфиденциальной информации (вида “ваша карта заблокирована”, “платеж на сумму зарегистрирован” и пр.), так как Банк осуществляет подобной рассылки.
10. В случае компрометации или подозрения на компрометацию ключей электронной подписи системы дистанционного банковского обслуживания незамедлительно обратиться в Банк для блокирования скомпрометированных ключей электронной подписи.
11. Использовать банкоматы, установленные в безопасных местах (в госучреждениях, подразделениях банков, крупных торговых комплексах, гостиницах, аэропортах и т.п.).
12. Не использовать банковские карты в организациях торговли и обслуживания, не вызывающих доверия.
13. Осуществлять информационное взаимодействие с Банком и другими кредитными организациями только с использованием средств связи (мобильные и стационарные телефоны, факсы, интерактивные WEB-порталы/сайты, обычная и электронная почта), реквизиты которых оговорены в документах, получаемых непосредственно в банке или других кредитных организациях.
14. Не подключать устройство, используемое для работы с системами дистанционного банковского обслуживания, к сетям общего доступа в местах свободного доступа в Интернет (Интернет-кафе, гостиницы, офисные центры и т.п.).

**ООО «Банк РСИ» рекомендует контролировать конфигурации устройств, используемых для работы с системами дистанционного банковского обслуживания:**

1. Система антивирусной защиты должна функционировать без сбоя все время использования устройства. Необходимо прекращать работу при сбое средств антивирусной защиты (в том числе в случае невозможности обновления баз данных сигнатур) до устранения сбоя и повторной проверки рабочего места на отсутствие вредоносного кода.
2. На устройстве не должно быть программного обеспечения неизвестного назначения
3. Необходимо прекращать работу с системой дистанционного банковского обслуживания, если изменился внешний вид системы, появились дополнительные элементы, при этом Банк не выполнял накануне работ по обновлению системы дистанционного банковского обслуживания
4. Необходимо прекратить работу с устройством, если нарушено функционирование межсетевых экранов, или имеются основания подозревать несанкционированный удаленный доступ к устройству, до момента устранения нарушения.

**ООО «Банк РСИ» рекомендует контролировать признаки возможного наличия вредоносного кода:**

1. Нарушается работа средств антивирусной защиты информации, невозможно обновить базу данных сигнатур, невозможно открыть только сайты разработчиков средств антивирусной защиты.
2. Нарушена работа средств межсетевого экранирования.
3. Установлено программное обеспечение неизвестного назначения без полномочий пользователя.
4. В пользовательских каталогах размещены файлы и каталоги, которые невозможно удалить.
5. Выполняются задачи неизвестного назначения без полномочий пользователя.
6. Средства антивирусной защиты сообщают об обнаружении вредоносного кода.