

Уважаемые клиенты!

АО «Россельхозбанк» (далее Банк) сообщает о возможных случаях мошеннических действий третьих лиц, связанных с:

- рассылкой в адрес клиентов ложных писем/уведомлений/ SMS-сообщений от лица Банка
- обзвоном клиентов от лица Банка

ПАМЯТКА КЛИЕНТАМ О СОБЛЮДЕНИИ БЕЗОПАСНОСТИ ПРИ ПОЛЬЗОВАНИИ ПРОДУКТАМИ И УСЛУГАМИ БАНКА

Для предотвращения мошеннических действий:

1. Соблюдайте правила личной цифровой безопасности:

- Не переходите по подозрительным ссылкам, полученным с использованием электронной почты или SMS-сообщений, в мессенджерах и социальных сетях. Не перезванивайте на указанные в сообщениях номера
- Сообщите Банку о смене номера мобильного устройства и в случае утраты мобильного устройства, так как ваши данные могут попасть к мошенникам
- При подозрении на компрометацию или утечку информации о персональных данных необходимо уведомить об этом Банк, а также незамедлительно произвести замену логина и пароля, используемых для «Мобильного банка» и/или «Интернет-банка»
- Используйте только официальные приложения Банка, загруженные из официальных магазинов приложений (например, в App Store, Google Play и пр.)

2. Не сообщайте никому, в том числе по телефону, конфиденциальную информацию:

- Реквизиты платежной карты (номер карты, срок действия карты, ПИН-код к карте, CVV/CVC-код, коды подтверждения из SMS-сообщений),
- Аутентификационные данные (в том числе логин и пароль) для входа в «Мобильный банк», «Интернет-банк» и пр.
- Свои персональные данные

3. Для безопасности платежных операций по картам в сети Интернет используется технология подтверждения операций специальным 3-D паролем. Банк по картам платежных систем VISA International, MasterCard WorldWide, МИР, JCB International/ международная платежная система UnionPay International осуществляет предоставление 3-D паролей на номер мобильного телефона, указанный Держателем карты для получения 3-D паролей при обращении в Банк/ в банкомате/ информационно-платежном терминале Банка. Срок действия 3-D пароля, полученного посредством SMS-сообщения, составляет 15 минут с момента его формирования и его действие распространяется только для одной операции, в процессе совершения которой данный 3-D пароль был получен.

4. Обращаем внимание на использование мошенниками ссылок для перехода на подменный сайт, замаскированный под сайт Банка/ лендинговые страницы с целью завладения персональными данными.

5. Запомните официальную информацию о Банке:


Официальные сайты Банка: www.rshb.ru | www.svoedom.ru

Существуют и используются злоумышленниками технологии подмены отображаемого на экране телефона номера **ВХОДЯЩЕГО** звонка. В случае сомнения, что входящий звонок осуществляется оператором Банка, необходимо завершить разговор и перезвонить по контактными данным Банка.

ВОПРОСЫ ПО МЕРАМ БЕЗОПАСНОСТИ МОЖНО ЗАДАТЬ В ЧАТЕ:



на сайте Банка
www.rshb.ru



в Мобильном приложении

Скачайте и установите бесплатно



Скачайте «Мобильный банк, Россельхозбанк» из App Store / Google Play



РоссельхозБанк