

**Уважаемые клиенты, АО «Россельхозбанк» сообщает о возможных случаях мошеннических действий третьих лиц, связанных с:**

- Рассылкой в адрес клиентов ложных писем, уведомлений, SMS-сообщений от лица Банков
- Обзвоном клиентов от лица Банков

**Памятка клиентам о соблюдении безопасности при использовании 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
- Не раскрывайте конфиденциальную информацию, в том числе персональные данные третьим лицам (номер платежной карты, срок действия платежной карты, ПИН-код к карте, CVV или CVC-код, коды подтверждения из SMS-сообщений, аутентификационные данные (в том числе логин и пароль) от «Мобильного банка», «Интернет-банка» и пр. (далее – Персональные данные)
- Не сообщайте никому персональные данные по телефону
- Сообщите банку о смене номера мобильного устройства или 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 «Интернет-банка»
- Используйте только официальные приложения Банка, загруженные из официальных магазинов приложений (например, в App Store, Google Play и пр.)

**2. Не вступайте с отправителями уведомлений в переписку, не переводите им денежные средства, не передавайте никакие документы, сведения, реквизиты и пр.**

**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 осуществляют 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:

- [www.rshb.ru](http://www.rshb.ru)
- <https://rshbdigital.ru/>

Сотрудники Банка никогда не запрашивают персональные данные и не дают указаний по телефону о необходимости проведения операций по переводу денежных средств на чужие карты, счета или номера мобильных телефонов.

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 контактному данным Банка.

---

При возникновении сомнений в том, что Вам звонят сотрудники Банка, или при возникновении вопросов рекомендуем обратиться за разъяснениями в любое отделение АО «Россельхозбанк» или по номеру телефона официального контакт-центра Банка **8-800-100-01-00**. При этом, обращаем внимание, что указанный номер предназначен только для приема входящих звонков, рассылка SMS-сообщений с него не осуществляется.

Вопросы по мере безопасности можно задать в чате:

- На сайте Банка (кнопка в правом нижнем углу)
- В мобильном приложении (кнопка в правом нижнем углу)