РУССКИЙ БАНК СБЕРЕЖЕНИЙ

общество с ограниченной ответственностью

ПАМЯТКА КЛИЕНТАМ БАНКА ООО «РУСБС»

о СОБЛЮДЕНИИ БЕЗОПАСНОСТИ

при пользовании банковскими картами, интернет-банком и другими услугами банка

Если Вам поступают звонки от имени «банковских работников» или SMS- сообщения, сообщения в социальных сетях и мессенджерах якобы от Банка ООО «РУСБС» (далее – Банк) с информацией, касающейся финансовых операций (подозрительный платеж (операция), сумма оплаты или Ваша карта заблокирована, проблемы с проведением операции, заблокирован доступ и т. п.):

✖ ни в коем случае не перезванивайте на указанные в сообщениях номера

✖ не сообщайте звонящим поступающие на телефон SMS-коды подтверждения и данные банковских карт: номер карты, срок действия, контрольный код с обратной стороны карты, а также персональные сведения: серия и номер паспорта, адрес регистрации

✖ прекратите контактировать и немедленно обратитесь в Банк по телефонам, которые указаны на оборотной стороне карты, на сайте Банка или в оригинальных банковских документах. Объясните оператору причину Вашего обращения.

При использовании карты в Интернете (особенно при привязке к регулярным платежам или аккаунтам) пользуйтесь только проверенными сайтами, т.к. велика вероятность перейти на поддельный сайт, созданный мошенниками для компрометации клиентских данных, включая платежные карточные данные.

При проведении операции в Интернете обращайте внимание на содержание SMS-сообщения с кодом подтверждения операции

Крайне важно самостоятельно обеспечить сохранность/конфиденциальность реквизитов своей карты и ПИН-кода (например, не пишите ПИН-код на самой карте и не передавайте карту третьим лицам).

Напоминаем, что операции по снятию наличных, совершенные с использованием ПИН-кода, считаются выполненными самим держателем карты и опротестованию не подлежат.

Если Вы выходите в Интернет через смартфон или планшет, настоятельно рекомендуем использовать антивирусное ПО. Это поможет минимизировать риск попадания в устройство вредоносных программ, предназначенных для перехвата приходящих от Банка SMS-сообщений, компрометации персональных данных и карточных авторизационных данных.

Не храните на своём устройстве средства доступа к системам дистанционного банковского обслуживания (логины и пароли), номера карт, паспортные данные и другую конфиденциальную информацию, чтобы она не стала доступна третьим лицам в случае утраты устройства.

При использовании мобильного телефона **соблюдайте следующие меры безопасности:** не подключайтесь к общедоступным Wi-Fi-сетям, не устанавливайте приложения из недостоверных источников, не открывайте подозрительные письма и ссылки