**Памятка по безопасному использованию банковских карт и**

**автоматизированной системы дистанционного банковского обслуживания "СББ-онлайн"**

ПАО "САРОВБИЗНЕСБАНК" предлагает своим клиентам продукты и услуги, отвечающие современным требованиям и стандартам. На наш взгляд, во многом безопасность использования банковских карт и систем дистанционного банковского обслуживания зависит от того, насколько ответственно держатель карты относится к вопросам обеспечения защиты персональной информации.

В настоящее время набирает популярность новый способ мошенничества, суть которого заключатся в том, что злоумышленники звонят на номер телефона клиента, называя его по имени и отчеству, представляются сотрудниками банка. После этого они сообщают, что по его банковской карте обнаружены подозрительные операции, и для их блокировки требуется назвать данные карты, трехзначный код, указанный на обороте карты, код из СМС или пароли от "СББ-онлайн". Получив данные сведения, злоумышленники направляют распоряжение от имени клиента для списания всех средств.

Что бы защитить себя от действий мошенников рекомендуем придерживаться следующих правил:

1. При поступлении с неизвестных номеров звонков или сообщений от имени "сотрудников службы безопасности банка" или якобы от "ПАО САРОВБИЗНЕСБАНК" (далее - Банк), в которых сообщается информация, касающаяся банковского обслуживания (*например, "ваша карта заблокирована", "заблокирована сумма оплаты" или "есть проблемы с проведением операции по Вашей карте" и т.п*.):

* **недопустимо сообщать реквизиты банковских карт**: полный номер карты, срок действия, трехзначный код действительности карты, указанный на обороте карты;
* **недопустимо разглашать одноразовые пароли (коды) из поступивших от банка СМС-сообщений;**
* недопустимо разглашать **персональные сведения**: серия и номер паспорта, адрес регистрации;
* **не перезванивать на указанные в сообщениях номера телефонов.**

1. Банк направляет информацию, касающуюся банковского обслуживания (например, коды подтверждения операций, сообщение о блокировке/разблокировке банковской карты и т.п.), только в сообщениях СМС/Push. Другие средства обмена сообщениями для передачи данной информации Банк **не использует**.
2. Работник **Банка никогда не звонит клиенту в процессе оплаты по карте, осуществлении перевода с карты или при использовании "СББ- онлайн"**. Не проводите действия в банкоматах и терминалах по инструкциям, полученным по телефону.
3. При вышеуказанных ситуациях, необходимо **сразу прекратить разговор**, и **самостоятельно обратиться в Банк** по телефону службы поддержки клиентов, указанному на оборотной стороне карты, на сайте Банка или в оригинальных банковских документах.
4. При использовании карты в интернете (особенно, в случае привязки карты к регулярным платежам или аккаунтам) **пользуйтесь только проверенными сайтами,** чтобы исключить вероятность перехода на мошеннический сайт.
5. При проведении операции в Интернете следует обращать внимание на **содержание СМС–сообщения с кодом подтверждения операции**, а именно: на место проведения операции (т.е. чтобы вместо наименования торговой точке не было указано "card2card" и т.п.), проверяйте сумму и вид платежа. Не вводите код из СМС, если есть расхождения в указанных параметрах проведения операции.
6. При разглашении реквизитов карты или кодов из СМС возможность в одностороннем порядке аннулировать перевод на карту/кошелек или оспарить операции не предусмотрена.
7. Владельцам мобильных устройств, используемых для совершения платежных операций через "СББ-онлайн", настоятельно рекомендуем **использовать и постоянно обновлять антивирусное программное обеспечение,** которое поможет уменьшить вероятность заражения мобильного устройства вредоносными программами.
8. Используйте только официальные банковские приложения из магазинов App Store, Google Play, Microsoft Store. **На мобильных устройствах, используемых для работы с "СББ-онлайн" не следует устанавливать приложения из недостоверных источников.**
9. Не прибегайте к взлому системы защиты устройства: Root (на платформе Android) и Jailbreak (на платформе iOS), это значительно повышает уязвимость вашего устройства для вредоносных программ.
10. При работе с беспроводными точками доступа не следует подключаться к общедоступным Wi-Fi-сетям.
11. При получении сообщений с просьбами для участия в розыгрыше предоставить реквизиты банковских карт, персональные данные или перейти по ссылке для получения каких-либо призов, следует игнорировать подобные сообщения и незамедлительно их удалять.
12. Рекомендуем написать заявление оператору мобильной связи о запрете принимать обращения на блокировку/разблокировку/замену СИМ–карты от третьих лиц по доверенности.

Будьте бдительны! Если Вы столкнулись с мошенниками, срочно звоните: в службу поддержки клиентов банка (контакт-центр) по телефону: 8-800-555-56-62 (круглосуточно, по России бесплатно).

июль 2019г.