

ПАМЯТКА

по безопасности при использовании удаленных каналов обслуживания по картам СберКарта с тарифным планом «Детский» ПАО Сбербанк

По тексту Памятки по безопасности при использовании Удаленных каналов обслуживания по картам Сберкарта с тарифным планом «Детский» ПАО Сбербанк используются термины и определения, содержащиеся в Договоре.

Вы присоединились к Договору, в рамках которого клиентам Банка предоставляется возможность совершать операции и получать информацию по счетам через Удаленные каналы обслуживания, к которым относятся:

- Устройства самообслуживания Банка,
- SMS-банк (Мобильный банк),
- Контактный Центр Банка.

Вы имеете возможность установить ограничение доступности (видимости) счетов, которые Вы не хотите использовать в Удаленных каналах обслуживания. Ограничение можно установить отдельно для каждого из каналов: для Устройств самообслуживания Банка и SMS-банка (Мобильного банка).

Правила пользования Удаленными каналами обслуживания определены в Договоре.

Использование Удаленных каналов обслуживания сопряжено с риском получения несанкционированного доступа к Вашей защищаемой информации с целью осуществления переводов денежных средств с Ваших счетов неуполномоченными лицами.

К защищаемой информации Клиента относится:

- информация об остатках денежных средств на счетах;
- информация о совершенных переводах денежных средств;
- информация, содержащаяся в оформленных Вами распоряжениях на перевод денежных средств;
- информация, необходимая для удостоверения Клиентами права распоряжения денежными средствами, в том числе данные Держателей карт;
- информация ограниченного доступа, в том числе персональные данные и иная информация, подлежащая обязательной защите в соответствии с законодательством Российской Федерации, обрабатываемая при осуществлении переводов денежных средств.

Ниже приведены рекомендуемые Банком меры по снижению рисков получения несанкционированного доступа к защищаемой информации Клиента.

Помните! Передача карты или ее реквизитов, Логина (Идентификатора пользователя), Постоянного пароля, Одноразовых паролей, Контрольной информации, предназначенных для доступа и подтверждения операций в Удаленных каналах обслуживания, другому лицу (в том числе работнику Банка) означает, что Вы предоставляете возможность другим лицам проводить операции по счетам.

При любых подозрениях на мошенничество, следует незамедлительно обратиться в Контактный Центр Банка по телефонам:

900
+7 (495) 500-55-50
8 (800) 555-55-50».

При обращении по указанным номерам телефонов происходит соединение с системой автоматизированного обслуживания (IVR). Для соединения с линией, предназначенной для передачи сообщения об утрате карты или о подозрении на мошеннические действия, необходимо в тоновом режиме набрать цифру «1».

Подробная информация о способах мошенничества и мерах защиты размещена на Официальном сайте.

Меры безопасности при использовании карты

Храните свою карту в недоступном для окружающих месте. Не передавайте карту и ее реквизиты другому лицу, за исключением продавца (кассира). Рекомендуется хранить карту отдельно от наличных денег и документов, удостоверяющих личность, особенно в поездках.

Во избежание мошенничества с использованием Вашей карты требуйте проведения операций с картой только в Вашем присутствии, не позволяйте уносить карту из поля Вашего зрения.

Не прислушивайтесь к советам третьих лиц, а также не принимайте их помощь при проведении операций. При необходимости обратитесь к сотрудникам в Подразделении Банка или позвоните по номерам телефонов, указанным на Устройстве самообслуживания или на оборотной стороне Вашей карты.

Во избежание использования Вашей карты третьим лицом храните ПИН отдельно от карты, исключив одновременный доступ к ним (например, в одном бумажнике), не пишите ПИН на карте, не сообщайте ПИН другим лицам (в том числе родственникам), не вводите ПИН при работе в сети Интернет.

Ни при каких обстоятельствах не сообщайте свой ПИН никому, включая сотрудников Банка.

Меры безопасности при работе с Устройствами самообслуживания

При проведении операции с вводом ПИНа ВСЕГДА прикрывайте клавиатуру, например, свободной рукой. Это не позволит мошенникам увидеть Ваш ПИН или записать его на видеокамеру.

Замки доступа по картам в специальные помещения, где устанавливаются Устройства самообслуживания, не должны требовать ввода ПИНа. Если для прохода в помещение от Вас требуется ввести ПИН, не делая этого, обратитесь в Банк. Если Вы ранее пытались воспользоваться подобным устройством, рекомендуем Вам срочно заблокировать карту, позвонив по номерам телефонов, указанным на Устройстве самообслуживания или на оборотной стороне Вашей карты, обратившись в Контактный центр Банка, независимо от того, получили ли Вы доступ к устройству или нет.

До проведения операции в Устройстве самообслуживания осмотрите его лицевую часть, в частности, поверхность над ПИН-клавиатурой и устройство для приема карты в Устройстве самообслуживания. В этих местах не должно находиться прикрепленных посторонних предметов или рекламных буклетов. При обнаружении подозрительных устройств, просим незамедлительно сообщить об этом сотрудникам Подразделения Банка, обслуживающим Устройство самообслуживания, или по номерам телефонов, указанным на Устройстве самообслуживания или

на оборотной стороне Вашей карты. Операцию с использованием карты для получения наличных в Устройстве самообслуживания в данном случае проводить не следует.

Не применяйте физическую силу, чтобы вставить карту в Устройство самообслуживания. Если карта не вставляется, воздержитесь от использования такого Устройства самообслуживания.

При приеме и возврате карты банкоматом не пытайтесь ускорить прерывистое движение карты в картоприемнике. Неравномерное движение карты является не сбоем, а необходимым средством защиты Вашей карты от компрометации.

Внимание! Не совершайте на Устройстве самообслуживания никаких операций по указаниям посторонних лиц, позвонивших Вам и представившихся работниками Банка или других организаций.

Меры безопасности для SMS-банка (Мобильного банка)

При утрате Мобильного устройства, используемого с абонентским номером подвижной радиотелефонной связи, на который предоставлен доступ к SMS-банку (Мобильному банку), Вам следует срочно обратиться к своему оператору сотовой связи для блокировки SIM-карты и в Контактный Центр Банка для приостановки действия SMS-банка (Мобильного банка).

При смене номера телефона, зарегистрированного для доступа к SMS-банку (Мобильному банку), Вам необходимо **немедленно** обратиться в Банк и сообщить о смене номера.

При внезапном прекращении работы SIM-карты необходимо срочно обратиться к своему оператору сотовой связи за уточнением причин – в отношении Вас возможно проведение мошеннических действий третьими лицами.

Будьте внимательны – не оставляйте свое Мобильное устройство без присмотра, не передавайте свое Мобильное устройство третьим лицам, чтобы исключить несанкционированное использование SMS-банка (Мобильного банка).

Своевременно устанавливайте доступные обновления операционной системы и приложений на Ваше Мобильное устройство. Используйте антивирусное программное обеспечение для Мобильного устройства, своевременно устанавливайте на него обновления антивирусных баз.

Не устанавливайте на свое Мобильное устройство нелегальные операционные системы, так как это отключает защитные механизмы, заложенные производителем мобильной платформы. В результате Ваше Мобильное устройство становится уязвимым к заражению вирусными программами.

Не переходите по ссылкам¹ и не устанавливайте приложения/обновления безопасности, пришедшие в SMS-сообщении или по электронной почте, в том числе от имени Банка.

Установите на Мобильном устройстве пароль для доступа к устройству, данная возможность доступна для любых современных моделей Мобильных устройств.

Защита от SMS -мошенничества

Мошеннические SMS-сообщения, как правило, информируют о блокировке Карты, о совершенном переводе средств или содержат другую информацию, побуждающую перезвонить на указанный в SMS-сообщении номер телефона для уточнения информации. Перезвонившему

¹ Не распространяется на ссылки, ведущие на Официальный сайт, полученные от Банка в SMS-сообщении с номера 900 для совершения сделки.

Клиенту мошенники представляются сотрудниками службы безопасности, специалистами службы технической поддержки банка и в убедительной форме предлагают срочно провести действия по разблокировке карты, по отмене перевода и т.п., в зависимости от содержания SMS-сообщения.

В случае получения подобных SMS-сообщений настоятельно рекомендуем Вам:

- не перезванивать на номер телефона, указанный в SMS-сообщении;
- не предоставлять информацию о реквизитах карты (номере карты, сроке ее действия, CVV2/CVC2/ППК2), ПИН, Контрольной информации, Одноразовых паролях, в т.ч. посредством направления ответных SMS-сообщений;
- не проводить через Устройства самообслуживания никакие операции по инструкциям, полученным по Мобильным устройствам.

В ряде случаев Банк рассылает информационные SMS-сообщения, при этом:

- в SMS-сообщениях, направляемых Банком по операциям, проведенным с использованием Вашей карты, обязательно указываются последние 4 цифры номера Вашей карты (мошенникам они не известны);
- SMS-сообщения Банка всегда отправляются с номера «900²», в них указываются только официальные номера телефонов Банка, опубликованные на Официальном сайте или указанные на Вашей Карте;
- SMS-сообщения Банка не рассылаются с официальных номеров телефонов Контактного Центра Банка +7 (495) 500-55-50 и 8 (800) 555-55-50.

Если полученное SMS-сообщение вызывает любые сомнения или опасения, необходимо обратиться в Контактный Центр Банка по официальным номерам телефонов, размещенным на оборотной стороне карты или на Официальном сайте.

В случае если Вы все же пострадали от SMS, необходимо:

- немедленно обратиться в Контактный Центр Банка по официальным номерам телефонов и заблокировать карту, реквизиты которой были сообщены мошенникам или по которой были совершены мошеннические операции;
- немедленно обратиться по телефону к оператору связи, в адрес которого переведены средства, с заявлением о мошенничестве и возврате средств (как правило, информация о номерах телефонов, на которые были переведены средства, сотовом операторе и номерах телефонов контактного центра сотового оператора указаны на чеке, полученном в Устройстве самообслуживания);
- подать через любое подразделение полиции заявление о совершенном мошенничестве на имя начальника управления «К» ГУВД\УВД.

Мошенничество через e-mail рассылки

Массовые мошеннические e-mail-рассылки, маскируясь под бренд ПАО Сбербанк, как правило, предназначены для:

- заманивания получателей сообщений на сайты-«ловушки», на которых под различными предложениями мошенники попытаются получить персональные и защищаемые данные (ФИО, Одноразовые пароли, Контрольную информацию, номера Карт и их сроки действия, ПИНЫ, CVV2/CVC2/ППК2 коды и пр. информацию). Часто на таких сайтах размещаются вирусы, заражающие компьютеры при открытии страниц;

² Указан основной номер, для разных регионов возможна также рассылка с номеров 9000, 9001, 8632, 6470, SBERBANK.

- принуждения под различными предложениями получателей писем на открытие файла-вложения, содержащего вирус, или переход по ссылке для загрузки вирусного файла.

Признаки того, что e-mail-сообщение является мошенническим:

- сообщения замаскированы под официальные письма Банка и требуют от Вас каких-либо быстрых действий или ответа;
- адрес отправителя и тема сообщения замаскированы под обращения от имени Банка.

Примеры наименования отправителей в мошеннических сообщениях:

Примеры тем сообщений в мошеннических рассылках:

- | | |
|--|---|
| <ul style="list-style-type: none"> – Сбербанк Онлайн (info@sber.ru) – Сбербанк России (noreply@sber.ru) – Сбербанк Информ (statistics@sber.ru) – и пр. | <ul style="list-style-type: none"> – «Сообщение об увеличении задолженности» – «Сообщение об увеличении долга» – «Сообщение об увеличении задолженности на ДД.ММ.ГГГГ» |
|--|---|
- письма содержат ссылки на интернет-ресурсы, похожие на официальные ресурсы Банка;
 - URL-адрес ссылки в письме отличается от официального адреса (www.sberbank.ru), возможно также появление всплывающих окон на официальном сайте, в котором запрашивается ввод или подтверждение Ваших персональных данных;
 - к сообщению прилагается файл-вложение, который Вам настойчиво рекомендуют открыть;
 - в тексте содержатся явные опечатки или орфографические ошибки.

Обращаем Ваше внимание, что ПАО Сбербанк никогда:

- не отправляет SMS-сообщения / не осуществляет телефонные звонки на мобильный телефон Клиента с просьбой подтвердить, обновить / предоставить ответным SMS-сообщением / звонившему на мобильный телефон персональные данные (ФИО, данные документа, удостоверяющего личность, номер мобильного телефона, информацию о номере Карты, сроке действия Карты, ППК2/CVV2/CVC2, ПИН, Контрольную информацию и пр.). **ОБРАЩАЕМ ВАШЕ ВНИМАНИЕ: ФИО ОБНОВЛЯЮТСЯ ТОЛЬКО ПРИ ЛИЧНОМ ПОСЕЩЕНИИ БАНКА ПО ПРЕДОСТАВЛЕНИИ ДОКУМЕНТА, УДОСТОВЕРЯЮЩЕГО ЛИЧНОСТЬ; РЕВИЗИТЫ ДОКУМЕНТА, УДОСТОВЕРЯЮЩЕГО ЛИЧНОСТЬ, ОБНОВЛЯЮТСЯ ПРИ ЛИЧНОМ ПОСЕЩЕНИИ БАНКА ПО ПРЕДОСТАВЛЕНИИ ДОКУМЕНТА, УДОСТОВЕРЯЮЩЕГО ЛИЧНОСТЬ;**
- не отправляет сообщения с формой для ввода Ваших персональных данных.