ПАМЯТКА
по безопасности при использовании удаленных каналов обслуживания ПАО Сбербанк

По тексту Памятки по безопасности при использовании удаленных каналов обслуживания 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,
- Сбербанк Онлайн,
- 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, для Сбербанк Онлайн (в том числе отдельно для мобильных приложений) и SMS-банка (Мобильного банка).

Установить или изменить перечень доступных счетов Вы можете как через Сбербанк Онлайн (по всем счетам), так и в любом Подразделении Банка на территории обслуживания соответствующего договора (только по счетам вкладов).

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 Банка.

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 в Сбербанк Онлайн

Для входа в Сбербанк Онлайн Вам необходимо ввести Логин (Идентификатор пользователя) и Постоянный пароль, дополнительно может вводиться Одноразовый пароль (если данная опция предусмотрена Вами при настройке «личной страницы»). Для входа в Сбербанк Онлайн не требуется вводить никакой другой информации (за исключением случая первоначальной регистрации в Сбербанк Онлайн на Официальном сайте Банка, когда для получения Логина (Идентификатора пользователя) и Постоянного пароля требуется ввести номер действующей банковской карты (кроме корпоративных карт)).

Внимание! Если для входа в Сбербанк Онлайн Вам предлагается ввести любую другую персональную информацию или дополнительные данные (номера карт[1], номер мобильного телефона, Контрольную информацию или другие данные), это указывает на мошенничество! В таких случаях необходимо немедленно прекратить сеанс работы в Сбербанк Онлайн и срочно обратиться в Банк.

Банк **никогда не запрашивает пароли для отмены операций** или шаблонов в Сбербанк Онлайн. Если Вам предлагается ввести пароль для отмены операции, в том числе и той, которую Вы не совершали, Вам необходимо прекратить сеанс работы в Сбербанк Онлайн и срочно обратиться в Банк.

При получении от Банка на Мобильное устройство SMS-сообщения и/или Push-уведомления с Одноразовым паролем внимательно ознакомьтесь с информацией в сообщении/уведомлении: все реквизиты операции в направленном Вам сообщении/уведомлении должны соответствовать той операции, которую Вы собираетесь совершить. Только после того как Вы убедились, что информация в этом SMS-сообщении/Push-уведомлении корректна, можно вводить пароль.

Используйте только надежные и проверенные точки Wi-Fi. Не рекомендуется подключаться к популярным и/или бесплатным точкам доступа Wi-Fi, если Вы не уверены в достоверности имени точки доступа. Обращаем Ваше внимание, что точки доступа Wi-Fi, для подключения к которым не требуется ввод пароля, могут представлять повышенную опасность в связи с возможными действиями мошенников, направленными на получение доступа к Вашим персональным данным.

Помните! Вводя Одноразовый пароль, Вы даёте Банку распоряжение о проведении операции с указанными в SMS-сообщении/Push-уведомлении реквизитами.

Ни при каких обстоятельствах не сообщайте Постоянный и Одноразовые пароли никому, включая сотрудников Банка.

В случае утери или кражи чека с Логином (Идентификатором пользователя) и Постоянным паролем Вам следует незамедлительно обратиться в Контактный Центр Банка.

[1] Указание номера карты требуется только при первоначальной регистрации в Системе «Сбербанк Онлайн».

При работе с Сбербанк Онлайн всегда проверяйте, что установлено защищенное ssl-соединение с официальным сайтом (https://online.sberbank.ru). В окне браузера должно быть изображение, обозначающее наличие защищенного соединения, которое отличается в зависимости от браузера. Как правило, в левой части адресной строки располагается замочек.

Не пользуйтесь Сбербанк Онлайн через Интернет-обозреватель Мобильного устройства, на который приходят SMS-сообщения/Push-уведомления с подтверждающим Одноразовым паролем. Для Мобильных устройств существуют специально разработанные Банком Мобильные приложения. Получить информацию о таких Мобильных приложениях Банка и способах их установки Вы можете на Официальном сайте Банка.

Для исключения компрометации Вашей финансовой информации и хищения средств, настоятельно не рекомендуем Вам подключать к услугам Банка номера телефонов, которые Вам не принадлежат.

Пользуйтесь дополнительными возможностями Сбербанк Онлайн по повышению уровня безопасности (SMS-информирование/Push-уведомления[2] о входе в Сбербанк Онлайн, настройка видимости карт и пр.). Для настройки используйте меню «Настройки», далее раздел «Настройки безопасности».

Не устанавливайте на Мобильное устройство, на которое Банк отправляет SMS-сообщения/Push-уведомления с подтверждающими Одноразовыми паролями, приложения по ссылкам, полученным от неизвестных Вам источников.

Помните, что Банк не рассылает своим клиентам ссылки или указания на установку Мобильных приложений через SMS/Push/MMS/e-mail–сообщения.

На Мобильных устройствах, которые Вы используете для доступа к Сбербанк Онлайн:

- используйте современное антивирусное программное обеспечение и следите за его регулярным обновлением;
- регулярно выполняйте антивирусную проверку для своевременного обнаружения вредоносных программ;
- своевременно устанавливайте обновления операционной системы, рекомендуемые компанией-производителем;
- используйте дополнительное лицензионное программное обеспечение, позволяющее повысить уровень защиты Вашего Мобильного устройства – персональные межсетевые экраны, программы поиска шпионских компонент, программы защиты от «СПАМ»-рассылок и пр.
- не используйте возможность войти в Систему «Сбербанк Онлайн» через Официальный сайт Банка по идентификационному файлу (cookie), если к устройству могут иметь доступ иные лица или удалите идентификационный файл (cookie) с устройства после завершения работы с Системой «Сбербанк Онлайн» одним из следующих способов:
  – выберите опцию «Сменить пользователя»[3] на странице входа в Систему «Сбербанк Онлайн»;
  – в браузере в разделе «Настройки», подразделе «Безопасность» выберите опцию «Очистить журнал обозревателя/журнал браузера/cookie»[4].Завершение работы с Сбербанк Онлайн выполняйте путем выбора соответствующего пункта меню.

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.

---

[2] При наличии технической возможности.
[3] Кнопка реализуется средствами программного обеспечения. Банк вправе изменять дизайн и наименование данной кнопки.
[4] Названия разделов и расположение данных опций зависят от используемого браузера.

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) и Мобильных приложений Банка

При утрате Мобильного устройства, используемого с абонентским номером подвижной радиотелефонной связи, на который предоставлен доступ к SMS-банку (Мобильному банку) или на которое установлено Мобильное приложение Банка, 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) и/или блокировки доступа в Сбербанк Онлайн.

При смене номера телефона, зарегистрированного для доступа к SMS-банку (Мобильному банку), Вам необходимо **незамедлительно** 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.

При подключении (регистрации) номера телефона для доступа к SMS-банку (Мобильному банку) по карте, Вам становится доступна возможность перевода денежных средств с Вашего счета дебетовой карты в адрес физических лиц, а также оплаты услуг юридических лиц посредством Запросов. Вы можете отключить данную возможность в любое время, отправив команду «НОЛЬ» на номер 900 или обратившись в Контактный Центр Банка.

Будьте внимательны – не оставляйте свое Мобильное устройство без присмотра, не передавайте свое Мобильное устройство третьим лицам, чтобы исключить несанкционированное использование SMS-банка (Мобильного банка) и Мобильных приложений Банка. Не переходите по ссылкам, полученным от Банка в Push-уведомлении в Мобильном приложении Банка, для подтверждения операции, если Вы не совершали данную операцию.

Используйте только официальные Мобильные приложения Банка, доступные в официальных магазинах приложений производителей мобильных платформ. Обязательно убедитесь, что в поле «разработчик мобильного приложения» указан ПАО Сбербанк.

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 нелицензионные 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 ссылкам[5] и не устанавливайте приложения/обновления безопасности, пришедшие в SMS-сообщении, Push-уведомлении 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.

[5] Не распространяется на ссылки, ведущие на Официальный сайт Банка или в Систему «Сбербанк Онлайн», полученные от Банка в SMS-сообщении с номера 900 для совершения сделки.

Не используйте Мобильное устройство для доступа к полнофункциональной версии Сбербанк Онлайн, для этого существуют специализированные Мобильные приложения, разработанные Банком.

Завершайте работу с Мобильным приложением Банка через завершение сессии (по кнопке «Выход»).

Защита от SMS/Push-мошенничества

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

В случае получения подобных SMS-сообщений/Push-уведомлений настоятельно рекомендуем Вам:

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

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

- в SMS-сообщениях/Push-уведомлениях, направляемых Банком по операциям, проведенным с использованием Вашей карты, обязательно указываются последние 4 цифры номера Вашей карты (мошенникам они не известны);
- SMS-сообщения/Push-уведомления Банка всегда отправляются с номера «900[6]», в них указываются только официальные номера телефонов Банка, опубликованные на Официальном сайте Банка или указанные на Вашей банковской карте;
- SMS-сообщения/Push-уведомления 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/Push-уведомление вызывает любые сомнения или опасения, необходимо обратиться в Контактный Центр Банка по официальным номерам телефонов, размещенным на оборотной стороне карты или на Официальном сайте Банка.

В случае если Вы все же пострадали от SMS/Push-мошенничества, 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 предлогами мошенники попытаются получить персональные и защищаемые данные (ФИО,

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

Логин (Идентификатор пользователя), Постоянный пароль, Одноразовые пароли, Контрольную информацию, номера банковских карт и их сроки действия, ПИНы, CVV2/CVC2/ППК2 коды и пр. информацию). Часто на таких сайтах размещаются вирусы, заражающие компьютеры при открытии страниц;

- принуждения под различными предлогами 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:

- Сбербанк Онлайн (info@sber.ru)
- Сбербанк России (noreply@sber.ru)
- Сбербанк Информ (statistics@sber.ru)
- и пр.

Примеры тем сообщений в мошеннических рассылках:

- «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 банковской 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, ИЛИ В МОБИЛЬНОМ ПРИЛОЖЕНИИ БАНКА[7];
- не отправляет сообщения с формой для ввода Ваших персональных данных;
- не просит Вас зайти в личный кабинет Сбербанк Онлайн по ссылкам в письмах.

[7] В Мобильном приложении Банка Клиент может самостоятельно изменить данные своего паспорта РФ: серия, номер, дата выдачи, код подразделения.