ПАМЯТКА
по безопасности при использовании карт

Храните свою карту в недоступном для окружающих месте. Не передавайте карту другому лицу, за исключением продавца (кассира). Рекомендуется хранить карту отдельно от наличных денег и документов, 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 работникам в филиале Банка или позвоните по телефонам, указанным на устройстве самообслуживания (УС) или на оборотной стороне Вашей карты.

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

Помните! Передача банковской карты или ее реквизитов, идентификаторов и паролей, предназначенных для доступа и подтверждения операций в системе «Сбербанк ОнЛ@йн», другому лицу (в том числе работнику Банка) означает, что Вы предоставляете возможность другим лицам проводить операции по Вашим счетам.

Внимание! Если Вы получили СМС-сообщение от Банка по операции, которую Вы не совершали, необходимо срочно заблокировать карту с помощью услуги «Мобильный банк», обратиться в Контактный центр Банка и следовать указаниям специалиста.

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

(495)-500-5550
800-555-5550

При обращении по указанным номерам телефонов происходит соединение с системой автоматизированного обслуживания. Для оперативного соединения со специалистом Банка для передачи сообщения об утрате карты или о подозрении на мошеннические действия, необходимо в тоновом режиме выбрать соответствующий пункт меню.

Рекомендуется заранее внести указанные номера в память Вашего телефона, чтобы оперативно обратиться в Контактный центр при необходимости.

Подробная информация о способах мошенничества и мерах защиты размещена на сайте Сбербанка России - www.sberbank.ru.

Меры безопасности при работе в системе «Сбербанк ОнЛ@йн»

Для входа в личный кабинет «Сбербанк ОнЛ@йн» Вам необходимо ввести идентификатор[1] и постоянный пароль, дополнительно может вводиться одноразовый пароль (если данная опция предусмотрена Вами при настройке «личной страницы»). Для входа в систему «Сбербанк ОнЛ@йн» не требуется вводить никакой другой информации.

Внимание! Если для входа в «Сбербанк ОнЛ@йн» Вам предлагается ввести любую другую персональную информацию или дополнительные данные (номер мобильного телефона, контрольную информацию по банковским картам или другие данные), это указывает на мошенничество! В таких случаях необходимо немедленно прекратить сеанс работы в системе «Сбербанк ОнЛ@йн» и срочно обратиться в Банк.

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

При получении от Банка СМС-сообщения с одноразовым паролем внимательно ознакомьтесь с информацией в сообщении: все реквизиты операции в направленном Вам сообщении должны соответствовать той операции, которую Вы собираетесь совершить. Только после того как Вы убедились, что информация в этом СМС-сообщении корректна, можно вводить пароль.

Помните! Вводя одноразовый СМС-пароль, Вы даёте Банку право и указание провести операцию с указанными в СМС-сообщении реквизитами.

Чек с одноразовыми паролями, распечатанный через устройство самообслуживания, храните отдельно от банковской карты и не передавайте третьим лицам, в том числе работникам Банка. Уничтожайте чеки с паролями, если Вы не планируете их использование.

Ни при каких обстоятельствах не сообщайте свои пароли никому, включая работников Банка.

---

[1] Если Клиент создал свой логин для входа в систему на странице входа в «Сбербанк ОнЛ@йн», то для входа можно использовать как идентификатор пользователя, так и логин, созданный Клиентом.

В случае утери или кражи чека Вам следует незамедлительно обратиться в Контактный Центр Банка или запросить новый список паролей в устройстве самообслуживания.

При работе с услугой «Сбербанк-ОнЛ@йн» всегда проверяйте, что установлено защищенное ssl-соединение с официальным сайтом услуги (**Ошибка! Недопустимый объект гиперссылки.**https://online.sberbank.ru). В окне браузера должно быть изображение, обозначающее наличие защищенного соединения, которое отличается в зависимости от браузера. Например, в браузере Microsoft Internet Explorer версия 8.0 в правой части адресной строки располагается желтый замочек, в более ранней версии – его изображение находится в правом нижнем углу экрана.

Не пользуйтесь услугой «Сбербанк ОнЛ@йн» через Интернет-обозреватель мобильного устройства (телефона, смартфона, планшета и пр.), на который приходят СМС-сообщения с подтверждающим одноразовым паролем. Для мобильных устройств существуют специально разработанные Банком приложения. Получить информацию о таких приложениях и способах их установки Вы можете на сайте Банка.

Для исключения компрометации Вашей финансовой информации и хищения средств, настоятельно не рекомендуется подключать к услугам Банка корпоративные номера телефонов и номера, которые Вам не принадлежат, в том числе по рекомендации третьих лиц, представившихся работниками Банка.

Не устанавливайте на мобильный телефон или иное устройство, на которое Банк отправляет СМС-сообщения с подтверждающими одноразовыми паролями, приложения по ссылкам, полученным от неизвестных Вам источников.

Внимание! На смартфонах и иных устройствах, подключенных к услугам «Мобильный банк» и «Сбербанк Онл@йн», Банк НАСТОЯТЕЛЬНО РЕКОМЕНДУЕТ использовать антивирусные программы, доступные в магазинах мобильных приложений, в том числе бесплатно.

Пользуйтесь возможностями системы «Сбербанк ОнЛ@йн» по повышению безопасности (СМС-информирование о входе, настройка видимости карт и прочее). Для настройки используйте меню «Настройки», далее пункт «Настройки безопасности».

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

На компьютерах, которые Вы используете для работы в «Сбербанк ОнЛ@йн»:

- используйте современное антивирусное программное обеспечение и следите за его регулярным обновлением;
- своевременно устанавливайте обновления операционной системы, рекомендуемые компанией-производителем;
- используйте дополнительное лицензионное программное обеспечение, позволяющее повысить уровень защиты вашего устройства – персональные межсетевые экраны, программы поиска шпионских компонент, программы защиты от «СПАМ» - рассылок и пр.;
- Завершение работы с системой выполняйте путем выбора соответствующего пункта меню.

Меры безопасности при работе с устройствами самообслуживания (УС)

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

Замки доступа по картам в специальные помещения, где устанавливаются УС, не должны требовать ввода ПИН-кода. Если для прохода в помещение от Вас требуется ввести ПИН-код, не делая этого, обратитесь в Банк. Если Вы ранее пытались воспользоваться подобным устройством, рекомендуем Вам срочно заблокировать карту, обратившись в Контактный центра Банка, независимо от того, получили ли Вы доступ к УС или нет.

До проведения операции в УС осмотрите его лицевую часть, в частности, поверхность над ПИН-клавиатурой и устройство для приема карты в УС. В этих местах не должно находиться прикрепленных посторонних предметов или рекламных буклетов. При обнаружении подозрительных устройств, просим незамедлительно сообщить об этом работникам филиала Банка, обслуживающим УС, или по телефонам, указанным на устройстве или на оборотной стороне Вашей карты. Операцию с использованием карты для получения наличных в УС в данном случае не проводить.

Не применяйте физическую силу, чтобы вставить банковскую карту в устройство. Если карта не вставляется, воздержитесь от использования такого УС.

При приеме и возврате карты устройством 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 УС никаких операций по указаниям посторонних лиц, позвонивших Вам и представившихся работниками Банка или других организаций. Помните! Вводя ПИН-код, Вы даёте Банку право и указание провести операцию, информация о которой отражена на экране УС.

Меры безопасности при работе с услугой «Мобильный банк» и мобильными приложениями «Сбербанк ОнЛ@йн» для смартфонов и планшетных устройств

Рекомендуется установить телефоне/смартфоне пароль для доступа к устройству, данная возможность доступна для большинства современных моделей устройств.

При утрате мобильного телефона или иного устройства, подключенного к услугам Банка, следует срочно обратиться к своему оператору сотовой связи для блокировки SIM-карты и в Контактный Центр Банка для приостановки действия услуг.

При смене номера телефона, на который подключена услуга «Мобильный банк» Вам необходимо **незамедлительно** обратиться в любое подразделение Банка и оформить заявление на отключение услуги «Мобильный банк» от старого номера телефона и на подключение услуги на новый номер телефона.

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

Внимание! В целях безопасности Банк может приостановить или ограничить действие услуг «Мобильный банк» и «Сбербанк ОнЛ@йн» при выявлении факта замены СИМ-карты по номеру телефона, подключенному к услугам Банка. В этом случае Вам необходимо обратиться в Контактный центра Банка и следовать указанием специалиста.

При подключении услуги «Мобильный банк», Вам становится доступна опция «Быстрый Платеж» - оплата любого номера мобильного телефона и пополнения счета Карты Банка по номеру телефона с Вашей банковской карты посредством СМС-сообщения. Если Вы не планируете использовать эту опцию, отправьте команду «НОЛЬ» на номер 900 или обратитесь в Контактный Центр Банка.

Будьте внимательны – не оставляйте свой телефон/устройство без присмотра, чтобы исключить несанкционированное использование услуг «Мобильный банк» и мобильных приложений «Сбербанк ОнЛ@йн».

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

Своевременно устанавливайте доступные обновления операционной системы и приложений на Ваш телефон/устройство.

Внимание! На смартфонах и иных устройствах, подключенных к услугам Банка, НАСТОЯТЕЛЬНО РЕКОМЕНДУЕТСЯ использовать антивирусные программы, доступные в магазинах мобильных приложений, в том числе бесплатно.

Не устанавливайте на свой телефон/устройство нелицензионные операционные системы, так как это отключает защитные механизмы, заложенные производителем мобильной платформы. В результате Ваш телефон становится уязвимым к заражению вирусными программами.

Не переходите по ссылкам и не устанавливайте приложения/обновления безопасности, пришедшие по СМС/электронной почте, в том числе от имени Банка.

Не используйте мобильный телефон для доступа к полнофункциональной версии услуги «Сбербанк-ОнЛ@йн», для этого существуют специализированные приложения, разработанные Банком.

Завершайте работу с мобильным приложением через соответствующий пункт меню.

Защита от СМС и e-mail мошенничества

Мошеннические СМС-сообщения, как правило, информируют о блокировке банковской карты, о совершенном переводе средств или содержат другую информацию, побуждающую перезвонить на указанный в СМС-сообщении номер телефона для уточнения информации. Затем мошенники представляются сотрудниками службы безопасности, специалистами службы технической поддержки и в убедительной форме предлагают срочно провести действия по разблокировке карты, по отмене перевода и т.п., в зависимости от содержания СМС-сообщения.

В случае получения подобных СМС-сообщений настоятельно рекомендуем Вам:

- не перезванивать на номер телефона, указанный в СМС-сообщении;
- не предоставлять информацию о реквизитах карты (номере карты, сроке ее действия, ПИН-коде, CVV2/CVC2 коде, контрольной информации по карте), или об одноразовых паролях, в т.ч. посредством направления ответных СМС-сообщений;
- не проводить через банкоматы и иные устройства самообслуживания никакие операции по инструкциям, полученным по телефону.

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

- в СМС-сообщениях, направляемых Банком по операциям, проведенным с использованием Вашей карты, обязательно указываются последние 4 цифры номера Вашей карты (мошенникам они не известны);
- СМС-сообщения Банка отправляются с номера «900[2]», в них указываются только официальные телефоны Банка, опубликованные на официальном сайте или указанные на оборотной стороне Вашей банковской карты.
- СМС-сообщения Банка не рассылаются с официальных номеров Контактного Центра Банка - 8-495-500-5550 и 8-800-5555550.

Если полученное СМС-сообщение вызывает любые сомнения или опасения, необходимо обратиться в Контактный Центр Банка по телефонам, указанным на обратной стороне банковской карты, и следовать указаниям специалиста.

Мошеннические e-mail-рассылки, маскируясь под бренд Сбербанка, как правило, предназначены для
заманивания получателей сообщений на сайты - «ловушки», на которых под различными предлогами мошенники попытаются получить персональные данные (идентификатор и пароль для входа в систему «Сбербанк-ОнЛ@йн», контрольную информацию по банковским картам, номера банковских карт, ПИН-коды, CVV и иную информацию) или принуждения под различными предлогами на открытие файла-вложения, содержащего вирус, или переход по ссылке для загрузки вирусного файла. Часто на таких сайтах размещаются вирусы, заражающие компьютеры при открытии страниц.

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. Например:

Примеры наименования отправителей в мошеннических сообщениях:	**Примеры тем сообщений в мошеннических рассылках:**
– Сбербанк ОнЛ@йн (info@sber.ru) – Сбербанк России (noreply@sber.ru) – Сбербанк Информ (statistics@sber.ru) – И другие	– «Сообщение об увеличении задолженности» – «Сообщение об увеличении долга» – «Сообщение об увеличении задолженности на ДД.ММ.ГГГГ»

- письма содержат ссылки на Интернет-сайты, похожие на официальные сайты Сбербанка;
- 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 Сбербанк России никогда:

- не отправляет сообщения с просьбой подтвердить, обновить или предоставить персональные данные (ФИО, данные документа, удостоверяющего личность, номер мобильного телефона, информацию банковской карты, CVV, ПИН-код, контрольную информацию и пр.);
- не отправляет сообщения с формой для ввода Ваших персональных данных;
- не просит Вас зайти в личный кабинет системы «Сбербанк ОнЛа@йн» по ссылкам в письмах.

Внимание! В случае если Вы все же пострадали от мошенничества:

1. Необходимо немедленно обратиться в Контактный Центр Банка для блокировки карты, реквизиты которой были сообщены посторонним или по которой были совершены несанкционированные операции, и следовать рекомендациям специалиста.
2. По факту мошенничества рекомендуется подать заявление в правоохранительные органы.

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