ТРАСТ | Банк

ПАМЯТКА ДЕРЖАТЕЛЯ БАНКОВСКОЙ КАРТЫ

Соблюдение приведенных ниже рекомендаций позволит обеспечить максимальную сохранность ваших денежных средств при использовании банковской карты как при совершении операций в банкоматах, так и безналичной оплате товаров и услуг, в том числе через сеть Интернет.

ХРАНЕНИЕ И ИСПОЛЬЗОВАНИЕ КАРТЫ

РЕКОМЕНДАЦИИ БАНКА	КАК ЭТО ПОМОЖЕТ?
При получении карты обязательно распишитесь на специально отведенной полосе на обороте карты.	Если злоумышленник завладеет картой и попытается совершить покупку в магазине, кассир обязан сверить подпись на карте и в паспорте предъявителя. На практике это делается редко, но снижает вероятность хищения ваших средств.
Категорически не рекомендуется указывать ПИН-код на самой карте – это все равно что класть деньги в дырявый карман. ПИН-код карты необходимо запомнить или сохранить в труднодоступном для третьих лиц месте.	В случае попадания вашей карты в чужие руки, злоумышленник сможет легко ею воспользоваться, сняв деньги в банкомате. ПИН-код – это аналог вашей подписи: указывая его на карте, вы выписываете чек на предъявителя.
Настоятельно рекомендуем не сообщать третьим лицам данные: срок действия, ПИН-код, секретный трехзначный код (CVC2/CVV2) вашей карты, в т.ч. когда вы ожидаете перевода денежных средств или если вам позвонили и назвались представителем какой-либо организации. Помните, что для совершения перевода отправителю необходимо и достаточно номера карты.	Такая просьба является тревожным сигналом, свидетельствующем о попытке совершения мошенничества: выяснив реквизиты карты, злоумышленник попробует воспользоваться ими сам или постарается убедить вас собственноручно перевести ему денежные средства (например, под видом тестовых операций, осуществления процедур разблокировки карты или возврата денежных средств после неуспешной операции). Маловероятно, что третье лицо попросит предоставить ключи доступа к карте (или счетам посредством Trust Online) в ваших интересах. Скорее всего, оправдывая просьбу желанием помочь, третье лицо попытается совершить хищение ваших средств. Даже при вашем личном обращении в офис Банка или при звонке по официальным телефонам работник Банка не имеет права спрашивать ПИН-код или секретные коды (CVC2/CVV2), напечатанные на оборотной стороне карты. При любой оплате в сети Интернет также не требуется вводить ПИН-код: если вас просят это сделать, то с большой долей вероятности под словом «ПИН» подразумевается не ПИН-код карты, а какой-то внутренний код, либо это попытка хищения данных.
Не рекомендуем отвечать на электронные письма и СМС-сообщения, в которых от имени Банка предлагается предоставить ваши персональные данные или данные вашей карты; следовать по ссылкам, указанным в таких сообщениях (включая ссылки на сайт Банка).	Банк не рассылает подобные сообщения, а злоумышленники с их помощью стремятся получить реквизиты вашей карты и иную конфиденциальную информацию. Ссылки могут вести на сайты-двойники, созданные для сбора указанной информации. Для консультации по любым вопросам предоставления услуг и продуктов Банка просим обращаться в офис Банка, либо по телефону горячей линии 8-800-200-11-44.

24 **8 800 200 1144**
Звонок по России бесплатный

8 495 587 9044
Для звонков из Москвы

WWW.TRUST.RU

Банк «ТРАСТ» (ПАО). 105066, Москва, ул. Спартаковская, д. 5, стр. 1.
Генеральная лицензия Банка России № 3279 от 26.08.2015.

Убедительно просим не передавать карту для использования третьим лицам, в том числе родственникам. Запомните, ваша карта – это ваш кошелек!	Даже без знания ПИН-кода без вашего ведома могут быть совершены операции: оплата через Интернет (достаточно реквизитов с самой карты) или безналичная оплата товаров /услуг, где вместо ПИН-кода предъявитель карты расписывается в чеке.
Регулярно делайте выписки по карте, контролируйте все операции, совершенные с использованием карты или ее реквизитов посредством Интернет-банка Trust Online, мобильного приложения Банка, а также услуги СМС-информирования.	Получая подробную информацию об операциях, вы своевременно узнаете о списании некорректной суммы, а также несанкционированных попытках списания денежных средств.
Если ваша карта была утрачена, вы обнаружили расхождение в сумме операции или у вас появились подозрения, что данные карты стали известны третьим лицам (например, на телефон приходят одноразовые пароли или СМС-сообщения о попытках/успешных операциях) – немедленно позвоните в Банк и заблокируйте карту. Сделать это можно круглосуточно через контакт-центр Банка, с использованием Интернет-банка Trust Online и услуги СМС-информирования (отправив СМС на номер 7588 вида < BLK[пробел]XXXX >, где XXXX – последние цифры номера карты).	Мошенники используют распределенные атаки для обхода систем безопасности Банка: совершают множественные попытки ввода данных по карте с целью подбора верных значений недостающих реквизитов (например, срока действия). Таким образом данные одной карты могут быть использованы на различных сайтах, а сбор данных может осуществляться частично, после чего возможно объединение реквизитов в единую цепочку в целях последующего совершения мошенничества.
Рекомендуем сохранить телефонный номер Банка в записной книжке для осуществления незамедлительной блокировки карты в случае ее утраты.	В случае утраты карты или при получении СМС о проведении операций, которые вы не совершали, вам не придется тратить значительное время, чтобы найти телефон Банка. Он понадобится и в случаях, когда «что-то пошло не так», когда возникли подозрения в мошеннических действиях. Сотрудники Банка по телефону окажут поддержку, ответят на вопросы.
В общественном транспорте старайтесь не держать карту в наружном кармане. Рекомендуем использовать специальный защитный (экранированный) чехол.	В людных местах (остановки, общественный транспорт) злоумышленник может попытаться провести бесконтактную оплату по карте, приблизив к вам терминал с введенной суммой оплаты на минимальную дистанцию, или просто украсть карту.
Установите в Интернет-банке Trust Online расходные лимиты по вашей карте. Доступны ограничения по типам операций, периоду (суточные и ежемесячные), месту нахождения (в РФ или за рубежом), а также по общему расходному лимиту.	Установка лимита по вашей карте позволит ограничить риск хищения денежных средств и соблюсти баланс между безопасностью и удобством. Если для совершения покупки потребуется большая сумма, лимит можно изменить в режиме онлайн.
Своевременно сообщайте Банку об изменении ваших персональных данных.	В целях обеспечения защиты ваших денежных средств Банк осуществляет мониторинг операций с использованием банковских платежных карт. Для минимизации риска проведения мошеннических операций и одновременно сохранения удобства использования платежного инструмента, крайне важно, чтобы Банк имел возможность оперативно связаться с вами.

24 **8 800 200 1144**
Звонок по России бесплатный

8 495 587 9044
Для звонков из Москвы

WWW.TRUST.RU

Банк «ТРАСТ» (ПАО). 105066, Москва, ул. Спартаковская, д. 5, стр. 1.
Генеральная лицензия Банка России № 3279 от 26.08.2015.

ТРАСТ | Банк

ОПЕРАЦИИ С КАРТОЙ (БАНКОМАТ, ТЕРМИНАЛ)

РЕКОМЕНДАЦИИ БАНКА	КАК ЭТО ПОМОЖЕТ?
Старайтесь совершать операции только в банкоматах известных банков (особенно за границей), расположенных в офисах, на территории административных зданий либо в охраняемой зоне под камерами видеонаблюдения. Особую бдительность проявляйте при пользовании банкоматами, расположенными на вокзалах, в аэропортах и торговых центрах.	Такие банкоматы хорошо просматриваются видеокамерами служб безопасности банков и правоохранительных органов, поэтому мошенники стараются туда не подходить. Небольшие считывающие устройства, которые устанавливаются злоумышленниками в банкоматах (скиммеры) способны считать данные вашей карты, необходимые для изготовления карты-дубликата. А миниатюрные видеокамеры запомнят вводимый вами ПИН-код. После чего с карты-дубликата мошенниками снимаются наличные средства.
Перед тем как воспользоваться банкоматом (особенно за границей), осмотрите его – изучите поверхность банкомата на предмет малозаметных отверстий, смысл которых не очевиден, потрогайте панели, клавиатуру.	Обычно фальшивые накладки, скрывающие вредоносные устройства злоумышленников, держатся плохо (а штатные детали таким образом не удастся повредить). Если что-то шатается, изучите деталь поближе или воспользуйтесь другим устройством – зачем рисковать?
При вводе ПИН-кода (в отсутствие специальных шторок) свободной рукой прикройте сверху клавиатуру.	Так вы максимально обезопасите себя от действий злоумышленников: даже в случае установки микрокамеры на банкомате (или вблизи кассы магазина), злоумышленники не получат ваш ПИН-код.
При оплате, особенно в кафе и барах, не позволяйте официанту (кассиру) уносить карту из вашего поля зрения; если необходимо – пройдите к терминалу оплаты вместе с ним.	С помощью мобильного считывающего устройства размерами со спичечный коробок подготовленный злоумышленник за несколько секунд получит копию вашей карты.
Не применяйте физическую силу, чтобы вставить карту в банкомат. Если карта не вставляется, воздержитесь от использования такого банкомата.	Затруднение при использовании карты в банкомате может быть связано с наличием в нем нештатного устройства или неисправностью банкомата.
После получения наличных денежных средств рекомендуем пересчитать банкноты, убедиться в том, что карта возвращена банкоматом, дождаться выдачи чека (если запрошен), затем спокойно все убрать обратно – и только после этого отходить от банкомата.	Спешка при обслуживании в банкоматах и инфокиосках часто приводит к утрате карты (которая может быть перехвачена злоумышленником) или несвоевременному обнаружению недостачи денежных средств.
При проведении операций с банковской картой в банкоматах рекомендуем не прислушиваться к советам третьих лиц, не принимать их помощь; при необходимости консультации, когда «что-то пошло не так» (не выдал деньги / не вернул карту), – обратиться к работнику Банка или позвонить по номеру контакт-центра.	Злоумышленник может спровоцировать ситуацию со сбоем устройства и воспользоваться вашим замешательством с целью хищения средств или получения конфиденциальных данных по вашей карте.

24 **8 800 200 1144**
Звонок по России бесплатный

8 495 587 9044
Для звонков из Москвы

WWW.TRUST.RU

Банк «ТРАСТ» (ПАО). 105066, Москва, ул. Спартаковская, д. 5, стр. 1.
Генеральная лицензия Банка России № 3279 от 26.08.2015.

ТРАСТ Банк

ОПЛАТА ЧЕРЕЗ СЕТЬ ИНТЕРНЕТ

РЕКОМЕНДАЦИИ БАНКА	КАК ЭТО ПОМОЖЕТ?
Избегайте покупок на подозрительных сайтах – сайтах малоизвестных организаций или недавно созданных, если наблюдаются сбои при обращении к разделам сайта, некорректное отображение данных, отсутствие обратной связи. Минимален риск мошенничества на сайтах с поддержкой технологии 3D-Secure (подтверждение операций одноразовым СМС-кодом, который вы получаете на мобильный телефон). Обращаем внимание, что при продаже товаров на популярных торговых площадках для получения оплаты вам достаточно сообщить только номер карты (иные данные карты не требуются).	Реквизиты карты могут быть перехвачены злоумышленниками с помощью специально созданных «однодневных» сайтов или сайтов-двойников для последующего совершения несанкционированных операций. При этом вам действительно может быть оказана услуга или продан товар.
Особенно внимательно отнеситесь к следующим рекомендациям: - своевременно обновляйте антивирусную защиту на устройстве, с которого осуществляется вход; - не храните крупные суммы денежных средств на карте (для крупных покупок безопаснее использовать отдельную карту); - используйте защищенный канал связи для выхода в Интернет (помните, неизвестная Wi-Fi сеть / сеть общего доступа в общественном месте не являются защищенными!); - работайте только со своего устройства; в случае использования стороннего устройства рекомендуем убедиться, что ваши персональные данные и информация о карте не сохранились (например, вновь загрузив в браузере web-страницу продавца, на которой совершались покупки).	Самый распространенный сценарий: на каком-либо сайте появляется окно с требованием обновить одно из приложений, потому что установленная на вашем устройстве версия устарела. Или появляется сообщение о том, что устройство заражено вирусами и его надо срочно проверить. Когда пользователь соглашается с обновлением, проверкой или просто переходит по ссылке, на его устройство загружается установочный файл вирусного приложения, и вирус получает доступ ко всем данным. Антивирус и ограничение излишних прав максимально повысят шансы на блокировку вредоносного ПО.
Скачивайте приложения на мобильный телефон и другие электронные устройства только с официальных источников (Google Play, iTunes Store, App Store).	Загружая приложения на сторонних сайтах, вы повышаете вероятность заражения устройства вирусом. В большинстве случаев вирусы попадают на устройство под видом каких-то безобидных приложений: браузеров, плееров, игр, книг и даже антивирусов.
Ограничьте излишние права на мобильном устройстве (права администратора).	Достаточно распространенным является уведомление о выигрыше электронной техники или денежного приза в лотерее. Вас попросят сообщить данные карты и другие персональные данные, после чего злоумышленники смогут осуществить хищение средств с вашей карты.
Не сообщайте третьим лицам одноразовый пароль, только что полученный по СМС от Банка. Работник Банка ни при каких обстоятельствах не спросит у вас одноразовый пароль. Если вам звонит неизвестное лицо и представляется сотрудником службы безопасности Банка или Банка России и при этом просит сообщить одноразовый пароль, полученный по СМС, – это точно мошенник!	Отправка одноразового пароля связана с действиями, подразумевающими использование реквизитов карты (в т.ч. с входом в Интернет-банк). Получив от вас одноразовый пароль, злоумышленники могут подтвердить проведение операции оплаты и успешно списать средства с вашей карты в сети Интернет.

24 **8 800 200 1144**
Звонок по России бесплатный

8 495 587 9044
Для звонков из Москвы

WWW.TRUST.RU

Банк «ТРАСТ» (ПАО). 105066, Москва, ул. Спартаковская, д. 5, стр. 1.
Генеральная лицензия Банка России № 3279 от 26.08.2015.