МЕРЫ БЕЗОПАСНОСТИ

Мы заботимся, чтобы проведение банковских операций было максимально безопасным. Однако надежность защиты невозможна без Вашего участия и соблюдения простых правил:

› Никому не сообщайте реквизиты карты: CVV2/CVC2-код (3-значный номер с обратной стороны карты), срок действия, а также одноразовые пароли для подтверждения операций. Сотрудники Банка никогда не запрашивают эти данные и не предлагают сообщить их «роботу»;

› Никому не сообщайте ПИН-код карты и не храните его вместе с картой;

› Если подозреваете, что карта скомпрометирована, позвоните нам по номеру 8-800-333-22-65 для ее блокировки. Заблокировать карту можно также в Личном кабинете;

› Не совершайте операции по указанию третьих лиц, в том числе по телефону. Не прислушивайтесь к советам третьих лиц, а также не принимайте их помощь при проведении операций с банковской картой;

› Не используйте незнакомые банкоматы, расположенные в затемненных, немноголюдных местах. Используйте банкоматы, которые расположены в офисах банков. На картоприемнике банкомата не должно быть посторонних предметов, клавиатура не должна шататься;

› Покупая в Интернете, убедитесь, что имеете дело с проверенным продавцом и используете его официальный сайт, а не сайт-подделку. Сайт должен использовать безопасный протокол https *(«замочек» в адресной строке браузера и символы https://);*

› Подтверждая Интернет-покупку, проверяйте реквизиты операции в сообщениях с одноразовым паролем — если реквизиты не совпадают, такой пароль использовать нельзя;

› На сайтах с объявлениями («Авито» и т. п.) во время общения с продавцом не сообщайте данные банковской карты, не переходите по ссылкам от продавца. Пользуйтесь услугой «Безопасная сделка»;

› Оплачивайте покупки банковской картой в Интернет только со своего компьютера или личного мобильного устройства;

› Устанавливайте расходные лимиты по операциям с картой, исходя из совершаемых/планируемых операций;

› Управляйте уровнем безопасности карты в Личном кабинете. Вы можете полностью запретить операции с картой в Интернет или установить на них ограничение;

› Подключайте и настраивайте удобные для Вас услуги по информированию об операциях по банковскому счету.

При возникновении вопросов, связанных с безопасностью Ваших средств, использованием карт или устройств самообслуживания БыстроБанка:

звоните 8-800-333-22-65

пишите clientsupport@bystrobank.ru

читайте https://www.bystrobank.ru/security/

ПАО «БыстроБанк», лицензия Банка России №1745. Реклама, 18.12.2024 г.

БыстроБанк

Безопасное использование

карт БыстроБанка

8-800-333-22-65
(по России звонок бесплатный)

www.bystrobank.ru

БыстроБанк выпускает банковские карты международной платежной системы Visa и российской национальной платежной системы Мир. Условия использования карт установлены в Правилах предоставления, обслуживания и использования банковских расчетных карт ПАО «БыстроБанк», которые размещены на сайте www.bystrobank.ru.

Карта VISA – это электронное средство платежа, которое принимается по всему миру.

Карта МИР – это электронное средство платежа, рабо-та которой не зависит от внешнеэкономических факторов.

УРОВНИ БЕЗОПАСНОСТИ КАРТЫ

Все виды карт Банка могут быть использованы для совершения операций в сети Интернет. Держатель карты самостоятельно определяет необходимый уровень безопасности расчетов:

Уровень	Описание
Только операции в электронных устройствах	Разрешены операции в банкоматах и торговых терминалах. Держатель карты не сможет совершать покупки в интернет-магазинах и любым другим способом, где не используется магнитная полоса и/или чип карты.
Все операции без ограничения лимита	Держатель карты может выполнять любые операции: и в банкоматах, и в Интернет. Операции проводятся в пределах остатка на счете.
Все операции с ограничением лимита	Держатель карты может выполнять любые операции, но, Банк дополнительно контролирует лимит операций, которые выполняются без чтения магнитной полосы и/или чипа карты. Данный уровень удобно использовать для разовых покупок в интернет-магазинах.

Уровни безопасности можно менять в офисе Банка или в Личном кабинете.

ПОДТВЕРЖДЕНИЕ ОПЕРАЦИЙ В ИНТЕРНЕТ

Банк использует технологию обеспечения безопасности платежей по банковским картам в сети Интернет 3-D Secure. При использовании этой технологии держатель карты подтверждает каждую операцию одноразовым паролем, который получает в виде SMS-сообщения от Банка (BystroBank) на мобильный телефон. НИКОМУ НЕ СООБЩАЙТЕ ЭТОТ ПАРОЛЬ!

ОГРАНИЧЕНИЯ НА ОПЕРАЦИИ (ЛИМИТЫ)

Для минимизации рисков Банком установлены лимиты на совершений операций с использованием карты с учетом типа совершаемых операций. Вы можете узнать актуальные лимиты и поменять их в офисе Банка или Личном кабинете.

ИНФОРМИРОВАНИЕ ОБ ОПЕРАЦИЯХ

Банк информирует клиентов об операциях по счету в соответствии с Правилами предоставления информации по счетам физических лиц в ПАО «БыстроБанк», которые размещены на сайте www.bystrobank.ru.

Мы советуем использовать услугу «SMS-оповещение о движении по счету» с нужными Вам настройками (с указанием или без указания остатка на счете, только расходные операции или все и т.д.) для оперативного информирования о любых операциях.

О РИСКАХ ВОВЛЕЧЕНИЯ В ДРОППЕРСТВО

› Законодательством предусмотрена ответственность за участие в дропперстве — деятельности по выводу и обналичиванию денежных средств, полученных преступным путем, в том числе с использованием электронных средств платежа;

› Банк применяет ограничения по операциям клиента, в отношении которого выявлены признаки дропперства;

› Не участвуйте в оформлении банковских карт и иных электронных средств платежа для третьих лиц, а также в проведении операций для них за вознаграждение;

› Не откликайтесь на объявления о легком заработке за деятельность по переводу денежных средств;

› Не откликайтесь на просьбы неизвестных Вам лиц принять перевод от «родственника», «друга» и обналичить его в банкомате (у получателя якобы повредилась карта и по иным подобным причинам);

› При поступлении неизвестного перевода свяжитесь с нами и опишите ситуацию;

› Игнорируйте входящие звонки с незнакомых номеров и сообщения от неизвестных лиц после получения подозрительного перевода;

› Не возвращайте «полученные по ошибке средства» переводом на другие счета;

› Помните, что «возврат ошибочного перевода» должен инициировать банк плательщика на основании обращения его клиента;

› Соблюдайте меры информационной безопасности для исключения возможности использования дропперами Ваших электронных средств платежа;

› Доводите данную информацию до Ваших близких, в особенности детей и родителей.

О РИСКАХ ЭЛЕКТРОННОГО СРЕДСТВА ПЛАТЕЖА

При использовании банковских карт следует учитывать риски получения мошенниками несанкционированного доступа к защищаемой информации — номеру и сроку действия карты, CVV2/CVC2-коду карты, а также кодам для подтверждения операций.

Компрометация вышеуказанной информации, в том числе предоставление ее третьим лицам по телефону, а также утеря карты, относятся к случаям повышенного риска.

В СЛУЧАЕ УТЕРИ ИЛИ КРАЖИ КАРТЫ НЕЗАМЕДЛИТЕЛЬНО ПОЗВОНИТЕ В БАНК 8-800-333-22-65 (КРУГЛОСУТОЧНО) И ЗАБЛОКИРУЙТЕ КАРТУ.