РИСКИ 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.

МЕРЫ БЕЗОПАСНОСТИ

Мы непрерывно заботимся о том, чтобы проведение банковских операций было максимально надежным и безопасным. Однако полная надежность защиты невозможна без Вашего участия и соблюдения Вами простых правил:

› Никому не сообщайте пароли для доступа на сайт, а также одноразовые пароли для подтверждения операций. Наши сотрудники никогда не запрашивают эти данные и не предлагают сообщить их «роботу»;

› Устанавливайте сложные длинные пароли и храните их в надежном месте. При использовании сертификатов защищайте их надежным мастер-паролем браузера;

› Настройте дополнительное подтверждение входа одноразовым паролем;

› Если подозреваете, что пароль или сертификат скомпрометирован, позвоните нам по номеру 8-800-333-22-65 для блокирования такого аналога собственноручной подписи;

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

› Пользуйтесь сайтом только со своих личных устройств, чтобы Вашими данными не воспользовались третьи лица;

› Проверяйте, что адресная строка сайта начинается с префикса https:// и Вы находитесь на официальном сайте bystrobank.ru;

› Защищайте свои устройства от посторонних с помощью блокировки сеанса пользователя на компьютере и блокировки экрана на мобильном устройстве;

› Используйте антивирус от заслуживающего доверия разработчика и устанавливайте обновления безопасности на все свои устройства;

› Не устанавливайте на Ваши устройства программы по просьбе третьих лиц. Наши сотрудники никогда не предлагают установить антивирус или другое стороннее приложение (для технической поддержки, защиты средств);

› Проверяйте реквизиты операции в сообщениях с одноразовым паролем — если реквизиты не совпадают, то такой пароль использовать нельзя;

› Подключайте и настраивайте удобные для Вас услуги по информированию об операциях, в том числе о входе с нового устройства;

› Управляйте персональными лимитами и ограничениями для онлайн-операций;

› О неполадках или необычном поведении сайта сообщайте нам на адрес clientsupport@bystrobank.ru.

звоните 8-800-333-22-65

пишите clientsupport@bystrobank.ru

читайте www.bystrobank.ru/security/

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

БыстроБанк

Безопасное использование

личного и бизнес кабинета

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

www.bystrobank.ru

ИСПОЛЬЗОВАНИЕ ЛИЧНОГО И БИЗНЕС КАБИНЕТА ПАО «БЫСТРОБАНК»

Кабинет позволяет из любой точки мира управлять счетами, вкладами и кредитами с использованием компьютера или смартфона.

Личный кабинет объединяет в себе инструменты для физических лиц, а Бизнес кабинет содержит инструментарий для юридических лиц.

Условия использования кабинета определяются Правилами удаленного банковского обслуживания и Правилами использования аналогов собственноручной подписи, которые доступны на сайте www.bystrobank.ru и в офисах Банка.

Для использования кабинета требуется только доступ в Интернет и современный браузер. Банк предоставляет различные способы входа в кабинет:

Способ входа (АСП)	Использование и возможности
Логин Банка	Создается вместе с паролем на сайте Банка. Регистрируется в офисе Банка или удаленно с использованием карты Банка или реквизитов договора. Присутствуют лимиты на операции.
ЕСИА	Создается на сайте Госуслуги. Позволяет владельцам подтвержденной учетной записи ЕСИА не запоминать дополнительные пароли и использовать механизмы безопасности и идентификации личности ЕСИА. Регистрируется удаленно, а также в офисе Банка. Присутствуют лимиты на операции.
Сертификат	Генерируется на сайте Банка, требует использования определенных браузеров. Регистрируется в офисе Банка. Лимиты на операции отсутствуют или высокие.

РЕКОМЕНДАЦИИ ПО ВЫБОРУ СПОСОБА ВХОДА

› Защищайте браузер надежным мастер-паролем (рекомендуем браузер Mozilla Firefox), независимо от способа входа. Надежность пароля зависит от его длины — используйте известные Вам фразы из книг или фильмов от 15 символов и больше.

› Рекомендуем использовать сертификат как самый безопасный способ для совершения платежных операций. Вы можете сделать резервную копию сертификата, защищенную надежным паролем, и хранить ее отдельно от основного устройства.

› Для использования кабинета на мобильных устройствах (смартфоны, планшеты) рекомендуем создавать отдельные учетные записи с правами только на просмотр или к отдельным счетам.

› Для максимальной безопасности Вы можете использовать несколько устройств и способов входа: одно для создания платежных документов, а другое для их отправки.

ОПОВЕЩЕНИЕ О ВЫПОЛНЕННОМ ВХОДЕ

Настройте уведомление о входе в кабинет и будьте в курсе, когда Ваши учетные данные используются для входа с нового устройства.

Каждый раз, когда совершается вход в Вашу учетную запись с нового устройства, мы будем присылать Вам сообщение с информацией, из какого браузера выполнен вход, в какое время это произошло и откуда.

Если вход с нового устройства совершен не Вами, незамедлительно обратитесь в Банк по телефону 8-800-333-22 65 для блокировки учетной записи.

ПОДТВЕРЖДЕНИЕ ОПЕРАЦИЙ И ВХОДА В КАБИНЕТ

Некоторые операции должны подтверждаться одноразовыми паролями, которые мы направляем на Ваши доверенные контакты (телефон или e-mail). Такие контакты обязательно должны быть верифицированы при регистрации АСП.

Настройте опцию «Подтверждение входа» в учетной записи в разделе «Безопасность». При каждом входе мы будем использовать дополнительный механизм проверки (доверенные контакты), чтобы убедиться, что именно Вы совершаете вход в кабинет.

ЛИМИТЫ И ОГРАНИЧЕНИЯ

Для минимизации рисков Банком устанавливаются базовые ограничения и лимиты на операции в системе.

Клиент вправе изменить базовые настройки по своим операциям. Для этого необходимо подать заявление в офисе Банка или в электронном виде.

Примеры изменяемых параметров:

› Возможность регистрации в кабинете с использованием реквизитов договора, реквизитов карты и путем авторизации в ЕСИА.

› Максимальная сумма перевода денежных средств за одну операцию и (или) в сутки.

› Максимальное число операций в сутки.

› Перечень услуг, предоставляемых с использованием системы удаленного обслуживания.

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 об операциях.

О РИСКАХ ЭЛЕКТРОННОГО СРЕДСТВА ПЛАТЕЖА

При использовании кабинета следует учитывать риски получения мошенниками несанкционированного доступа к защищаемой информации — Вашему логину, паролю, к ключам сертификата, а также кодам для подтверждения операций.

Компрометация указанной информации, в том числе предоставление ее третьим лицам (по телефону или иначе), относится к случаям повышенного риска.

В СЛУЧАЕ ПОЛУЧЕНИЯ ТРЕТЬИМИ ЛИЦАМИ ИНФОРМАЦИИ О ВАШЕМ ЛОГИНЕ И ПАРОЛЕ, КЛЮЧЕ СЕРТИФИКАТА, ОДНОРАЗОВОМ ПАРОЛЕ ДЛЯ ПОДТВЕРЖДЕНИЯ ОПЕРАЦИИ НЕЗАМЕДЛИТЕЛЬНО ПОЗВОНИТЕ В БАНК 8-800-333-22-65 (КРУГЛОСУТОЧНО).