Как безопасно пользоваться услугами Paysera?

Система Paysera всецело защищена, однако безопасность учетной записи и данных также зависит от ваших действий в интернете. Ниже представленные рекомендации помогут вам обезопасить ваши действия в интернете в целом и в учетной записи Paysera в частности.

Учетная запись

Вы можете подключиться к системе Paysera через мобильное приложение (введя пароль или с используя биометрические данные) или через браузер.

Чтобы подключиться через браузер:

1. Зайдите на сайт https://www.paysera.com, нажмите *ВОЙТИ*, и вы будете перенаправлены на страницу подключения https://bank.paysera.com/ru/login.
2. Выберите способ идентификации: электронная почта или номер телефона, - и введите данные.

3. Выберите способ подключения к учетной записи:

- через мобильное приложение. В этом случае в приложении нужно будет подтвердить контрольный код (он должен совпадать с кодом, отображенным в окне браузера). Откройте приложение Paysera и проведите пальцем по полоске подтверждения, если отображенный на экране подключения код совпадает с кодом в приложении. Для большей безопасности рекомендуем использовать для идентификации при подключении к приложению «Touch ID» или «Face ID».

- с помощью пароля. Введя пароль, вы войдете в свою учетную запись и сможете просматривать информацию по счету, но другие функции будут недоступны. Чтобы полноценно управлять своей учетной записью, вам нужно будет подтвердить подключение: в меню слева нажмите *Аутентификация* и выберите её способ – через мобильное приложение или с помощью SMS-сообщения. Пожалуйста, учитывайте то, что за услугу SMS-сообщения взимаются дополнительные сборы.

#

#

При подключении к учетной записи через браузер помните о нескольких очень важных правилах безопасности:

- откройте в браузере новое окно и введите адрес https://www.paysera.x (вместо «x» могут быть введены только следующие домены: **lt**, **com**, **lv**, **bg**, **ee**, **pl**, **es**, **de**, **ro**, **al**, **ge**). В правом верхнем углу нажмите ВОЙТИ, и вы будете перенаправлены на страницу https://bank.paysera.com/ru/login. Убедитесь в том, что соединение шифруется (в адресной строке виден замок, адрес начинается с «https», и в конце есть буква «s» – в некоторых случаях она видна только после нажатия на адресную строку), а для безопасного соединения используется выданный исключительно Paysera электронный сертификат, как показано на картинке.

Система недоступна по другим – хотя и очень похожим – адресам, таким как www.payssera.com, bank.paysera.anotherdomain.com, paysera.myf1ntech.com/paysera/login и пр.

Если вы открыли сайт, используя подобный адрес, и он очень похож на официальный сайт Paysera, скорее всего, вы попались на удочку мошенников. В таком случае не вводите никакие данные и незамедлительно свяжитесь с Центром обслуживания клиентов Paysera.

- всегда выходите из учетной записи, окончив работу с ней. Избегайте подключения к интернет-банку со сторонних устройств, поскольку на них могут быть установлены запоминающие пароль и другие данные программы.
- рекомендуем проверять IP-адреса, с которых осуществлялось подключение к вашей учетной записи, хотя бы раз в месяц. Для этого выберите Настройки > Настройки учетной записи > История подключений. Если у вас возникли какие-либо сомнения, проверьте, осуществлялись ли какие-то операции и подключения с использованием другого IP-адреса. В системе Paysera клиент может установить IP-адреса, с которых можно подключаться к его учетной записи. Для этого выберите Настройки > Настройки учетной записи > Дополнительные меры безопасности. Если у вас возникли подозрения относительно того, что к вашей учетной записи могли подключаться посторонние лица, незамедлительно свяжитесь с Центром обслуживания клиентов Paysera.
- не сообщайте никому данные для подключения к учетной записи. Если кто-то предложил вам открыть счет Paysera от своего или чьего-то еще имени или же осуществить какие-то финансовые операции, свяжитесь с Центром обслуживания клиентов, и вам скажут, что делать.
- обновляйте свою личную информацию и контактные данные, как только они изменились. В случае инцидента, связанного с безопасностью, или для того, чтобы сообщить вам важную информацию, сотрудникам Paysera может понадобиться незамедлительно связаться с вами и/или идентифицировать вас должным образом.
- новоиспеченным клиентам Paysera следует обратить внимание на «Анкету клиента». На картинке справа показано, как она выглядит в приложении Paysera.

Напоминаем, что, связавшись с вами, сотрудники Paysera никогда не будут просить вас предоставить коды подключения или подтверждения операций или пароли для входа в систему. Наши сотрудники могут попросить вас предоставить определенные данные подключения **только для установления вашей личности** и только если вы **сами обратились в службу поддержки клиентов**. Если у вас возникли сомнения в том, что с вами связался сотрудник Paysera, рекомендуем попросить его перезвонить вам позже и самим связаться со службой поддержки клиентов по указанным на нашей странице контактам.

#

Пароль учетной записи

Пароль для подключения к учетной записи должен быть уникальным и состоять не менее чем из 8 символов, включая заглавные и строчные буквы, цифры и специальные символы.

Пожалуйста, не используйте в пароле информацию о себе и своих близких (например, даты рождения, имена и фамилии членов семьи и друзей, клички животных или комбинации цифр и букв, которые легко угадать).

Постарайтесь запомнить пароль и не храните его в записной книжке, телефоне или ещё где-то. Рекомендуем использовать специальные программы-хранилища для паролей и зашифровать ваш пароль.

Не используйте один и тот же пароль в разных системах, так как он может быть использован в том числе для подключения к вашей учетной записи Paysera. Если у вас возникли подозрения относительно того, что ваш пароль могли узнать посторонние лица, незамедлительно смените его и проверьте, не было ли несанкционированных подключений к вашей учетной записи, неподтвержденных вами платежных операций с использованием вашего счета или попыток их осуществить.

Рекомендуется менять пароль каждые 3-6 месяцев.

Напоминаем, что **Paysera не отправляет писем с требованием сменить пароль**. Даже если Paysera сообщает о возможных угрозах вашим данным или учетной записи или же о необходимости совершить какие-то действия, в сообщении **никогда не будет ссылки**, перейдя по которой, клиент окажется на странице для смены пароля. Также Paysera никогда не предлагает клиентам загрузить прикрепленные файлы, установить программное обеспечение или сообщить коды подключения. Получив подозрительное сообщение, обратитесь в службу поддержки клиентов.

#

Смарт-устройства

Пользуйтесь только легально импортированными и приобретенными устройствами с оригинальным лицензированным программным обеспечением и мобильными приложениями, скаченными только в «Google Play» и «App Store».

Когда устройство не используется, оно должно быть заблокировано с помощью специального кода, пароля и т.п. Код блокировки устройства и PIN-код приложения Paysera не должны совпадать с частями вашего номера телефона, номера машины и даты рождения или состоять из комбинаций цифр, которые легко угадать – все коды должны быть уникальными. Также рекомендуем использовать «Touch ID» или «Face ID».

Предустановленное и иное программное обеспечение должно обновляться сразу после того, как его производитель объявил о выпущенном обновлении. Обновления предназначены для устранения недостатков, связанных как с функциональностью программы, так и с безопасностью. Поэтому они являются одной из гарантий безопасности операций, осуществляемых с использованием вашего устройства.

На всех устройствах, которые Вы используете для подключения к учетной записи Paysera, установите антивирусные программы. Мы также рекомендуем установить (особенно на компьютерах) межсетевой экран (англ. *firewall*), который не позволит подключиться к устройству по интернету.

#

Другие действия в интернете

Будьте бдительны, когда предоставляете свои данные в интернет-пространстве — убедитесь, что сайт надежный.

Перед совершением покупок в интернете проверьте репутацию и рейтинг продавца на форумах и других сайтах. На ненадежность интернет-магазина может указывать только что зарегистрированное название (домен) сайта, а также отсутствие у компании реального названия, кода регистрации и контактной информации. Обратите внимание и на адрес сайта: убедитесь в том, что он начинается с http**s**:// и что в нем есть буква «s».

Интернет-магазины часто предлагают оплатить покупки картой с требованием указать ее данные. Совершайте покупки на сайтах, на которых доступны специальные логотипы, подтверждающие безопасность платежей: «3-D Secure», «Verified by Visa» или «Mastercard SecureCode».

Не нажимайте на неизвестные или замаскированные (т.е. сокращенные, со скрытым источником) ссылки в социальных сетях, SMS-сообщениях и электронных письмах. Также не открывайте неизвестные документы, не устанавливайте программное обеспечение из неизвестных источников и не посещайте небезопасные сайты.

#

#

Сертифицированная безопасность

Безопасность системы Paysera подтверждает её соответствие международному стандарту безопасности данных индустрии платежных карт PCI DSS (англ. Payment Card Industry Data Security Standard). Данный стандарт регламентирует требования к компаниям, принимающим платежи картами и обрабатывающим данные клиентов. Система Paysera соответствует наивысшему стандарту безопасности (1 уровня), позволяющему безопасно осуществлять более 6 миллионов операций по картам в год.

#

В любой вызывающей подозрения ситуации (получив подозрительное сообщение от имени Paysera, заметив сомнительные операции в выписке по счету, потеряв данные для подключения или поняв, что вы ввели их на ненастоящем сайте, и т.п.), незамедлительно обратитесь в службу поддержки клиентов Paysera. Мы всегда поможем найти выход!