

Памятка по информационной безопасности для клиентов Финансовой Платформы Маркетплейс.

ПАО Московская Биржа, как Оператор Финансовой Платформы Маркетплейс, доводит до вашего сведения, что использование Удаленных каналов обслуживания сопряжено с риском получения несанкционированного доступа к конфиденциальной информации Клиента и осуществления несанкционированных переводов денежных средств со счетов неуполномоченными лицами.

К конфиденциальной информации Клиента относятся:

- информация об остатках денежных средств на счетах;
- информация о совершенных переводах денежных средств;
- информация, содержащаяся в оформленных Клиентом распоряжениях на перевод денежных средств;
- информация, необходимая для удостоверения Клиентами права распоряжения денежными средствами,
- информация ограниченного доступа, в том числе персональные данные и иная информация, подлежащая обязательной защите в соответствии с законодательством Российской Федерации, обрабатываемая при осуществлении переводов денежных средств.

Оператор Финансовой Платформы не несет ответственности за безопасность каналов связи, программах и аппаратных средств, которые используются Пользователями для доступа к Сайту Платформы Личному кабинету.

В связи с этим для минимизации рисков при работе с Платформой рекомендуется соблюдение следующих правил.

1. Используйте лицензионное программное обеспечения
2. Следите за своевременным обновлением операционных систем на используемых вами устройствах
3. Используйте современное антивирусное программное обеспечение, следите за его регулярным обновлением и регулярно выполняйте антивирусную проверку для своевременного обнаружения вредоносных программ.
4. Не открывайте неизвестные файлы, присланные на email: в них, могут содержаться трояны и другие вредоносные программы.

5. Не переходите по неизвестным ссылкам, присланным на email или через соцсети: они могут вести на зараженные сайты.
6. Не устанавливайте программы, скачанные из недоверенных источников
7. Не заходите в Личный кабинет Платформы с компьютера или иного устройства, которое использует для подключения к интернету недоверенную wi-fi сеть.
8. Никогда не передавайте третьим лицам логин, пароль и иную информацию, которую они могут использовать для несанкционированного доступа к Личному кабинету Платформы и исключить иные возможности получения указанной информации третьими лицами.
9. Не храните пароль к Личному кабинету Платформы в текстовых файлах на компьютере или флешке, а также используйте для входа в кабинет пароль, отличный от пароля для входа на устройство с которого вы осуществляете операции.
10. Не используйте функцию автозаполнения в установках вашего браузера. Это поможет не сохранять данные (пароль пользователя, имя пользователя и др.) в памяти браузера, что, в свою очередь, предотвратит использование данных сторонними лицами.
11. Регулярно меняйте пароли для доступа к Личному Кабинету.
12. Для исключения компрометации Вашей финансовой информации и хищения средств не используйте для целей подтверждения проведения операций на Платформе номер телефона, который официально вам не принадлежит.
13. При утрате Мобильного устройства, используемого с абонентским номером подвижной радиотелефонной связи, на который предоставлен доступ к Платформе Вам следует срочно обратиться к своему оператору сотовой связи для блокировки SIM-карты и в Контактный Центр Оператора Электронной Платформы для приостановки действия доступа в Личный кабинет Платформы.
14. При смене номера телефона, зарегистрированного для доступа к Платформе, Вам необходимо незамедлительно обратиться в Контакт центр и сообщить о смене номера.
15. Не передавайте телефон с SIM-картой, с которого осуществляется доступ к системе, во временное пользование посторонним лицам.
16. Ни при каких обстоятельствах не сообщайте Постоянный и Одноразовые пароли доступа никому, включая сотрудников Оператора Электронной Платформы.

17. Внимательно следите за содержанием электронных сообщений с разовыми паролями доступа. Если такие сообщения вызывают сомнения необходимо обратиться в Контактный Центр Оператора Электронной Платформы

Обращаем Ваше внимание, что Оператор Финансовой Платформы никогда:

- не отправляет сообщения с просьбой подтвердить, обновить или предоставить персональные и конфиденциальные данные (ФИО, Логин, Идентификатор пользователя, Постоянный пароль, Одноразовые пароли, Контрольную информацию, номера счетов и банковских карт и сроки их действия, ПИНЫ, CVV2/CVC2/ППК2 коды, Код клиента, данные документа, удостоверяющего личность, номер мобильного телефона и пр. информацию).
- не отправляет сообщения с формой для ввода Ваших персональных данных;
- не просит Вас зайти в Личный кабинет клиента по ссылкам в письмах.

При получении подобных сообщений, а также подозрениях на несанкционированные операции следует незамедлительно обратиться в Контакт центр Оператора Финансовой Платформы.