Финуслуги
Платформа личных финансов

Памятка
по информационной безопасности
для клиентов Финуслуг

1. ПАО Московская Биржа, как оператор финансовой платформы (далее – Оператор), доводит до вашего сведения, что использование удаленных каналов обслуживания сопряжено с риском получения несанкционированного доступа к конфиденциальной информации Участника финансовой платформы и осуществления несанкционированных переводов денежных средств со счетов неуполномоченными лицами.

2. К конфиденциальной информации Участника финансовой платформы относится:

- информация об остатках денежных средств на счетах;
- информация о совершенных переводах денежных средств;
- информация, содержащаяся в оформленных распоряжениях на перевод денежных средств;
- информация, необходимая для удостоверения 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.

3. Оператор не обеспечивает безопасность каналов связи, программных и аппаратных средств, которые используются для получения доступа к сайту Оператора в информационно-телекоммуникационной сети «Интернет» и личному кабинету Участнику финансовой платформы.

4. В целях минимизации рисков при работе с платформой Финуслуги рекомендуем соблюдать следующие правила.

1) Подключите второй фактор аутентификации пользователя для вашей учетной записи ЕСИА. Инструкцию по подключению второго фактора аутентификации вы можете найти в своем личном кабинете на Портале государственных услуг Российской Федерации (gosuslugi.ru);

2) Используйте лицензионное программное обеспечение на используемых Вами устройствах;

3) Следите за своевременным обновлением операционных систем на используемых Вами устройствах;

4) Используйте современное антивирусное программное обеспечение, следите за его регулярным обновлением и регулярно выполняйте антивирусную проверку для своевременного обнаружения вредоносных программ;

5) Не открывайте неизвестные файлы, присланные по электронной почте (email): в них, могут содержаться трояны и другие вредоносные программы;

6) Не переходите по неизвестным ссылкам, присланным электронной почте (email) или через социальные сети: они могут вести на зараженные сайты;

7) Не устанавливайте программы, полученные из недоверенных источников, используйте только лицензионное программное обеспечение, скаченное с официальных ресурсов;

8) Не заходите в личный кабинет платформы Финуслуги с компьютера или иного устройства, которое использует для подключения к информационно-телекоммуникационной сети «Интернет» недоверенную wi-fi сеть.

9) Никогда не передавайте третьим лицам логин, пароль и иную информацию, которую они могут использовать для несанкционированного доступа к вашему личному кабинету на платформе Финуслуги и исключить иные возможности получения указанной информации третьими лицами.

10) Не храните пароль к личному кабинету платформы Финуслуги (учетные данные для доступа на Портал gosuslugi.ru) 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.

11) 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.

12) Регулярно меняйте пароли для доступа к личному кабинету платформы Финуслуги.

13) Для исключения компрометации Вашей финансовой информации и хищения средств не используйте для целей подтверждения проведения операций на платформе Финуслуги номер телефона, который официально вам не принадлежит (зарегистрирован на другое лицо).

14) При утрате мобильного устройства, используемого с абонентским номером подвижной радиотелефонной связи, на который предоставлен доступ к платформе Финуслуги Вам следует срочно обратиться к своему оператору сотовой связи для блокировки SIM-карты и в контактный центр Оператора (Обратная связь finuslugi.ru) для приостановки действия доступа в личный кабинет платформы Финуслуги.

15) При смене номера телефона, зарегистрированного для доступа в личный кабинет на платформе Финуслуги, Вам необходимо незамедлительно обратиться в Контакт центр и сообщить о смене номера.

16) Не передавайте телефон с SIM-картой, с которого осуществляется доступ к сайту платформы Финуслуги в информационно-телекоммуникационной сети «Интернет» или к мобильному приложению, во временное пользование посторонним лицам.

17) Ни при каких обстоятельствах не сообщайте постоянный и одноразовые пароли доступа никому, включая сотрудников Оператора.

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

5. Обращаем Ваше внимание, что Оператор никогда:

- не отправляет сообщения с просьбой подтвердить, обновить или предоставить аутентификационные данные и финансовую информацию (ФИО, Логин, идентификационные данные или иные реквизиты учетной записи пользователя, постоянный пароль, одноразовые пароли, контрольную информацию, номера счетов и банковских карт и сроки их действия, ПИНы, CVV2/CVC2/ППК2 коды, и пр. информацию).
- не отправляет сообщения с формой для ввода Ваших персональных данных;
- не просит Вас зайти в личный кабинет платформы Финуслуги по ссылкам в письмах.

При получении подобных сообщений, а также при возникновении подозрений о совершении несанкционированных операций следует незамедлительно обратиться в Контакт центр Оператора.

Телефоны: 8 (800) 505–32–32 +7 (495) 145–32–32.

Электронная почта: service@finuslugi.ru