УТВЕРЖДЕНО
Приказом Генерального директора
Акционерного общества
«Универсальные Финансовые Технологии»
№ 1/КЛ от «20» марта 2024 г.

ПРАВИЛА

ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ КЛИЕНТОВ ПЛАТФОРМЫ АКЦИОНЕРНОГО ОБЩЕСТВА «УНИВЕРСАЛЬНЫЕ ФИНАНСОВЫЕ ТЕХНОЛОГИИ»

2024

СОДЕРЖАНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящий документ описывает правила по информационной безопасности для пользователей финансовой платформы АО “Универсальные финансовые технологии” (далее – Оператор). Оператор доводит до сведения, что использование удаленных каналов обслуживания сопряжено с риском получения несанкционированного доступа к конфиденциальной информации получателя финансовых услуг и осуществления несанкционированных переводов денежных средств со счетов неуполномоченными лицами.

2. КОНФИДЕНЦИАЛЬНАЯ ИНФОРМАЦИЯ КЛИЕНТА

К конфиденциальной информации получателя финансовых услуг Оператора относится информация ограниченного доступа, в том числе персональные данные и иная информация, подлежащая обязательной защите в соответствии с законодательством Российской Федерации, обрабатываемая при осуществлении операций финансовой платформы.

3. БЕЗОПАСНОСТЬ КАНАЛОВ СВЯЗИ

Оператор не обеспечивает безопасность каналов связи, программных и аппаратных средств, которые используются для получения доступа получателями финансовых услуг к сайту Оператора в информационно-телекоммуникационной сети “Интернет” и личному кабинету получателя финансовых услуг финансовой платформы.

4. МИНИМИЗАЦИЯ РИСКОВ

В целях минимизации рисков, при работе с финансовой платформой, рекомендуем соблюдать следующие правила:

- Настройте двухфакторную аутентификацию для вашей учетной записи ЕСИА. Инструкцию по настройке вы можете найти на Портале государственных услуг Российской Федерации (gosuslugi.ru);
- Используйте лицензионное программное обеспечение на используемых вами устройствах;

- Следите за своевременным обновлением операционных систем на используемых вами устройствах;
- Используйте современное антивирусное программное обеспечение, следите за его обновлением и регулярно выполняйте антивирусную проверку для своевременного обнаружения вредоносных программ;
- Не открывайте неизвестные файлы, присланные по электронной почте (email): в них, могут содержаться трояны и другие вредоносные программы;
- Не переходите по неизвестным ссылкам, присланным электронной почте (email) или через социальные сети: они могут вести на зараженные сайты;
- Не устанавливайте программы, полученные из не доверенных источников, используйте только лицензионное программное обеспечение, скаченное с официальных ресурсов;
- Не заходите в личный кабинет финансовой платформы с компьютера или иного устройства, которое использует для подключения к информационно-телекоммуникационной сети «Интернет» не доверенную WI-FI сеть;
- Никогда не передавайте третьим лицам логин, пароль и иную информацию, которую они могут использовать для несанкционированного доступа к вашему личному кабинету на финансовой платформе и исключить иные возможности получения указанной информации третьими лицами;
- Не храните пароль к личному кабинету финансовой платформы в текстовых файлах на компьютере или внешних носителях информации, а также используйте для входа в кабинет пароль, отличный от пароля для входа на устройстве, с которого вы осуществляете операции;
- Не используйте функцию автозаполнения в установках вашего браузера. Это поможет не сохранять данные (пароль, имя и др.) в памяти браузера, что, в свою очередь, предотвратит использование данных сторонними лицами;
- Регулярно меняйте пароли для доступа к личному кабинету финансовой платформы;
- Для исключения компрометации вашей финансовой информации и хищения средств не используйте для подтверждения проведения операций на финансовой платформе номер телефона, который официально вам не принадлежит (зарегистрирован на другое лицо);
- При утрате мобильного устройства, используемого с абонентским номером подвижной радиотелефонной связи, на который предоставлен доступ к финансовой платформе Вам следует срочно обратиться к своему оператору сотовой связи для

блокировки SIM-карты и в контактный центр Оператора для приостановки действия доступа в личный кабинет финансовой платформы;

- При смене номера телефона, зарегистрированного для доступа в личный кабинет на финансовой платформе, Вам необходимо незамедлительно обратиться в контактный центр и сообщить о смене номера;
- Не передавайте телефон с SIM-картой, с которого осуществляется доступ к сайту финансовой платформы в информационно-телекоммуникационной сети «Интернет» или к мобильному приложению, во временное пользование посторонним лицам;
- 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.

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, ПИН коды, CVV2/CVC2/ППК2 коды, и пр. информацию);
- Не отправляет сообщения с формой для ввода ваших персональных данных;
- Не просит Вас зайти в личный кабинет финансовой платформы по ссылкам в электронных письмах.

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

Телефон Горячей линии: +7-800-555-49-94

Электронная почта: uft@fin-id.ru