КСП КАПИТАЛ УПРАВЛЕНИЕ АКТИВАМИ

УТВЕРЖДЕНЫ
Приказом
Генерального директора
КСП Капитал УА ООО
№278 от 20 декабря 2019 года

Рекомендации по информационной безопасности при использовании информационного сервиса «Личный кабинет»

Уважаемые пользователи!

Общество с ограниченной ответственностью «КСП Капитал Управление Активами» (далее – «Управляющая компания») считает своим долгом заботу о вашей безопасности и безопасности ваших вложений. Специалисты Управляющей компании прилагают все усилия и применяют комплекс различных мер для обеспечения высокого уровня конфиденциальности, целостности и доступности активов клиентов Управляющей компании.

Настоятельно просим вас при использовании информационного сервиса «Личный кабинет» (далее – «Сервис») соблюдать базовые правила информационной безопасности, изложенные ниже.

Рекомендации по использованию Сервиса

Логины и пароли для работы в Сервисе – это ваша персональная конфиденциальная информация. Ни при каких обстоятельствах не раскрывайте свой логин и пароль никому, включая сотрудников Управляющей компании.

При обращении от имени кого-либо по телефону, электронной почте, посредством СМС-сообщений с просьбами сообщить конфиденциальную информацию (пароли, идентификаторы доступа, одноразовые коды подтверждения, полученные в СМС-сообщениях, и т.д.), ни при каких обстоятельствах не следует сообщать такую информацию.

Используется только защищенное соединение. Стандартно для такого рода соединения браузеры отображают в адресной строке соответствующий значок с закрытым замком зеленого цвета. Убедитесь, что соединение установлено именно с официальным сайтом Сервиса https://kspcapital-am.ru. Настоятельно не рекомендуется переходить на данную страницу по ссылкам с Интернет-ресурсов (за исключением официального ресурса Управляющей компании) или поступивших по электронной почте писем.

Управляющая компания отправляет СМС-сообщения только с использованием имен «KSPCapital» или «KSP Capital». Всегда проверяйте корректность наименования отправителя.

Обращайте внимание на любые изменения в привычных для вас процессах установления соединения или в функционировании Сервиса. При возникновении сомнений в правильности функционирования Сервиса, а также при подозрении на нестабильность работы Сервиса, следует незамедлительно прекратить его использование и обратиться в отдел по работе с клиентами Управляющей компании по номеру +7-495-649-88-37.

После окончания использования Сервиса обязательно корректно завершите работу, выйдя из Системы с использованием кнопки «Выход», даже в том случае, если вы авторизуетесь с помощью портала «Госуслуги».

При использовании авторизации с помощью пароля используйте только надежные пароли и регулярно их меняйте - пароли должны удовлетворять требованиям сложности и не должны повторяться в течение 24 месяцев. Не устанавливайте пароли, используемые в ваших учетных записях других информационных систем.

Не сохраняйте ваш логин и пароль в текстовых файлах на жестком диске компьютера, либо на других электронных носителях информации, так как в указанных случаях существует риск их кражи и компрометации.

Рекомендации по использованию программного обеспечения

Установите и регулярно обновляйте лицензионное антивирусное программное обеспечение на вашем компьютере. Действие вирусов может быть направлено на перехват вашей персональной информации и передаче её злоумышленникам.

Своевременно устанавливайте обновления операционной системы своего компьютера, рекомендуемые компанией-производителем в целях устранения выявленных в нем уязвимостей. Регулярно выполняйте обновления операционной системы и браузера вашего компьютера, так как данные действия значительно повысят его уровень безопасности.

Установите и настройте персональный брандмауэр (firewall) на вашем компьютере, что позволит вам запретить несанкционированный удаленный доступ к вашему компьютеру из сети «Интернет» и вашей локальной сети. Такое программное средство присутствует в базовом составе программного обеспечения операционной системы Microsoft Windows, а также обычно входит в состав антивирусного программного обеспечения.

Используйте дополнительное программное обеспечение, позволяющее повысить уровень защиты вашего компьютера: программы поиска шпионских компонент, программы защиты от спам-рассылок.

Не используйте на локальном компьютере без действительной необходимости учетную запись с административными правами.

Исключите посещение с вашего компьютера сайтов сомнительного содержания и любых других Интернет-ресурсов (социальные сети, форумы, чаты, телефонные сервисы и т.д.), а также чтение почты и открытие почтовых документов от недостоверных источников.

Категорически не рекомендуется использовать Сервис из мест, не заслуживающих доверия (интернет-кафе) или с использованием общественных каналов связи (бесплатный Wi-Fi и т.п.), так как это существенно увеличивает риск кражи ваших персональных данных.

По вопросам работы Сервиса и получения технической консультации вы можете обращаться в отдел по работе с клиентами Управляющей компании по контактам, указанным на официальном сайте Управляющей компании http://kspcapital-am.ru.