КАПИТАЛ LIFE
СТРАХОВАНИЕ ЖИЗНИ

Памятка по информационной безопасности для клиентов КАПИТАЛ LIFE

Информация о возможных рисках получения несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления.

Данный документ подготовлен в соответствии с требованиями Положения «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций» (утв. Банком России 20.04.2021 г. № 757- П).

Общество с ограниченной ответственностью «Капитал Лайф Страхование Жизни» (далее – КАПИТАЛ LIFE) доводит до Вашего сведения:

- информацию о возможных рисках получения несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления;
- информацию о мерах по предотвращению несанкционированного доступа к защищаемой информации, в том числе при утрате (потере, хищении) клиентом устройства, с использованием которого им совершались действия в целях осуществления финансовой операции, контролю конфигурации устройства, с использованием которого клиентом совершаются действия в целях осуществления финансовой операции, и своевременному обнаружению воздействия вредоносных программ.

Риск-ориентированный принцип, используемый КАПИТАЛ LIFE при взаимодействии с клиентами, подразумевает участие клиентов в реализации требований, нацеленных на выявление и снижение последствий от рисков, связанных с применением средств автоматизации, в частности:

- рисков несанкционированного доступа и уничтожения информации;
- рисков трансформации настроек программного обеспечения;
- рисков, связанных с неправильной обработкой информации;
- рисков совершения юридически значимых действий, влекущих возникновение, изменение либо прекращение прав и обязанностей по договорам страхования;
- рисков финансовых потерь.

В последнее время участились случаи мошенничества в интернете, направленные на обман пользователей. Чтобы защитить себя от злоумышленников, следуйте этим простым рекомендациям:

1. Не передавайте личные данные. Никогда не сообщайте третьим лицам свои персональные данные, такие как номер паспорта, СНИЛС, ИНН, реквизиты банковских карт, пароли к личным кабинетам, SMS-коды и другие конфиденциальные сведения.

   КАПИТАЛ LIFE никогда не запрашивает такую информацию через электронную почту или мессенджеры.

2. Проверяйте подлинность сайта и приложений. Перед тем как вводить личные данные на сайте или в приложении, убедитесь, что Вы находитесь на официальном ресурсе страховой компании КАПИТАЛ LIFE – www.kaplife.ru. Проверьте адрес сайта в адресной строке окна браузера – он должен начинаться с «https://» и содержать название компании без ошибок. Избегайте переходов по ссылкам из подозрительных писем или сообщений.

   Рекомендуем в браузере сохранить в Избранное или Закладки адрес сайта КАПИТАЛ LIFE (https://kaplife.ru) и адрес Кабинета клиента КАПИТАЛ LIFE (https://lk.kaplife.ru).

3. Для скачивания мобильного приложения «Мобильный Кабинет клиента» используйте Qr-код или ссылки размещённые на сайте КАПИТАЛ LIFE на странице «Мобильный кабинет клиента». Адрес страницы: https://kaplife.ru/app

4. Будьте осторожны с письмами, сообщениями в мессенджерах и звонками.

   Мошенники могут отправлять письма и инициировать общение в мессенджерах якобы от имени страховой компании или ее представителей с требованием предоставить личную информацию или оплатить штраф/комиссию. В таких письмах строка «Отправитель» может содержать похожий адрес электронной почты и отличатся от официального только на один символ.

Не переходите по ссылкам и не открывайте файлы в электронных письмах от неизвестных Вам отправителей.

Помните, что КАПИТАЛ LIFE не требует срочной оплаты через электронные кошельки или банковские переводы. Если у Вас возникают сомнения, свяжитесь с нашей службой поддержки по официальному номеру телефона – 8 800 200-68-86, 0911 (для звонков с мобильных).

5. Используйте сложные пароли. Установите сложный пароль для использования Кабинета клиента КАПИТАЛ LIFE на сайте КАПИТАЛ LIFE в сети Интернет https://kaplife.ru и мобильного приложения «Мобильный Кабинет клиента» (приложение доступно для бесплатного скачивания в магазинах приложений: Google Play, App Store и AppGallery).

   Пароль должен содержать не меньше 8 символов и представлять собой комбинацию из букв латинского алфавита (заглавные или строчные буквы) и цифр. Разрешается использовать специальные символы, имеющиеся на клавиатуре (например, символы: ! @ # $ % ^ & * [ ] ( ) » « % . , : ; / \ | ? ~ ` ‘ “ + - = – _< >). Ваш пароль не должен содержать логин от Кабинета клиента. Запрещается использовать в качестве пароля легко вычисляемые слова и комбинации. Пароль должен быть уникальным и использоваться только в Кабинете клиента КАПИТАЛ LIFE.

6. Запомните свой пароль либо используйте специальное программное обеспечение для хранения паролей в зашифрованном виде. Не записывайте и не храните свой пароль в открытом доступе.

7. Для входа в Кабинет клиента КАПИТАЛ LIFE или мобильное приложение используйте функцию «Войти через Госуслуги».

8. Обеспечьте безопасность учетной записи своей электронной почты и учетной записи на портале «Госуслуги». Это поможет Вам в случае необходимости восстановить доступ, в том числе в случае утраты персонального мобильного устройства.

9. Не заходите в Кабинет клиента КАПИТАЛ LIFE со случайных компьютеров, например, из интернет-кафе или других непроверенных мест.

10. Не используйте для доступа к сети Интернет общедоступный Wi-Fi, не требующий логина и пароля. Такой Wi-Fi злоумышленники используют для «внедрения» с помощью специальных программ в поток передачи информации и перехвата личных данных: логинов, паролей, номеров телефона. Такой Wi-Fi злоумышленники могут маскировать под сети ресторанов, отелей, аэропортов. Подключаться к таким сетям означает открыть свои данные.

    В случаях, когда использование общедоступного Wi-Fi является вынужденным, или в поездках за границей, используйте VPN. Выбирайте надежного VPN-провайдера, например, поставщика Вашего антивирусного ПО.

11. Используйте браузеры с поддержкой российских сертификатов: Яндекс Браузер или Атом. Если Вам удобно использовать другой браузер, Вы можете установить сертификат НУЦ Минцифры России на Ваше устройство. Для этого зайдите на портал Госуслуги и воспользуйтесь инструкцией по установке сертификата Минцифры https://www.gosuslugi.ru/crt

12. Сообщайте о подозрительной активности. Если Вам кажется, что кто-то пытается Вас обмануть, немедленно свяжитесь с нашей службой поддержки по официальному номеру телефона - 8 800 200-68-86, 0911 (для звонков с мобильных). Мы всегда готовы помочь Вам разобраться в ситуации и принять меры для защиты Ваших данных.

Рекомендации для защиты Вашего персонального компьютера и мобильного устройства – это поможет предотвратить заражение Вашего устройства вредоносными программами, которые могут украсть Ваши данные:

- используйте только лицензионное программное обеспечение;
- устанавливайте все необходимые обновления безопасности, рекомендуемые производителем программного обеспечения;
- устанавливайте лицензионное антивирусное программное обеспечение. Антивирусное программное обеспечение должно регулярно обновляться, желательный промежуток времени — 1 раз в 4-6 часов. Рекомендуем настроить по умолчанию максимальный уровень политики безопасности, не требующий ответов пользователя при обнаружении зараженных объектов. Лечение и удаление зараженных объектов должно производиться в автоматическом режиме;
- настройте полную антивирусную проверку Ваших устройств не реже 1 раза в неделю в автоматическом режиме. Такую проверку возможно настроить по расписанию, когда устройство включено, но Вами не используется, например, ночью;
- не загружайте программы и данные из непроверенных источников, не посещайте сайты сомнительного содержания.

Помните, Ваша безопасность – наша общая забота. Следуя этим простым правилам, Вы сможете избежать неприятностей и сохранить свои средства и личные данные в безопасности.