

## **Рекомендации по защите информации при использовании каналов удаленного обслуживания ООО СК «Эверия Лайф»**

Вы заключили Договор личного страхования (далее - «Договор») с ООО СК «Эверия Лайф» (далее - «Общество»), в рамках которого Страхователям предоставляется возможность совершать операции и получать информацию по Договору с использованием каналов удаленного обслуживания, к которым относятся:

- Официальный сайт Общества <https://everialife.ru/> (далее - «Официальный сайт»);
- Личный кабинет страхователя <https://my.everialife.ru/> (далее - «ЛК»);
- Мобильное приложение для страхователя [Everia Life Client](#) (Android, Google Play), [Everia Life Client](#) (Apple iOS, App Store) и [Everia Life Client](#) (Android, AppGallery) (далее - «Мобильное приложение»);
- Контактный центр [8 \(800\) 775 82 00, +7 \(495\) 785 82 00.](tel:88007758200)

Использование каналов удаленного обслуживания сопряжено с риском получения несанкционированного доступа к конфиденциальной информации Страхователя (далее - «Защищаемая информация»), риском ее разглашения, риском внесения изменения в Ваши регистрационные данные, а также осуществления переводов денежных средств, не связанных с оплатой по Договору, неуполномоченными лицами. К Защищаемой информации относятся:

- информация о совершенных переводах денежных средств;
- информация, содержащаяся в оформленных Вами распоряжениях на перевод денежных средств;
- информация, необходимая для удостоверения Вами права распоряжения денежными средствами, в том числе данные Держателей карт;
- 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.

Ниже приведены рекомендуемые Обществом меры по снижению рисков получения несанкционированного доступа к конфиденциальной информации Клиента.

**Помните! Передача карты или ее реквизитов, Постоянного пароля, Одноразовых паролей, предназначенных для доступа и подтверждения операций в каналах удаленного обслуживания, другому лицу (в том числе работнику Общества) означает, что Вы предоставляете возможность другим лицам проводить операции по Договору.**

При любых подозрениях на противоправные действия (если Вы получили SMS-сообщение/Push-уведомление от Общества по операции, которую Вы не совершали, или которое вызывает любые сомнения и опасения), следует незамедлительно обратиться в Контактный центр Общества по указанным в Договоре или на Официальном сайте Общества номерам телефонов:

**8 (800) 775-82-00,  
+7 (495) 785-82-00.**

### **Меры безопасности при использовании банковской карты**

Храните свою банковскую карту (далее – «карту») в недоступном для окружающих месте. Не передавайте карту и ее реквизиты другому лицу, за исключением продавца (кассира). Рекомендуется хранить карту отдельно от наличных денег и документов, удостоверяющих личность, особенно в поездках.

Во избежание противоправных действий с использованием Вашей карты требуйте проведения операций с картой только в Вашем присутствии, не позволяйте уносить карту из поля Вашего зрения.

Не прислушивайтесь к советам третьих лиц, а также не принимайте их помощь при проведении операций. При необходимости обратитесь к сотрудникам банка в подразделении банка или позвоните по номерам телефонов, указанным на оборотной стороне Вашей карты.

Во избежание использования Вашей карты третьим лицом храните ПИН отдельно от карты, исключив одновременный доступ к ним (например, в одном бумажнике), не пишите ПИН на карте, не сообщайте ПИН другим лицам (в том числе родственникам), **не вводите ПИН при работе в сети Интернет.**

**Ни при каких обстоятельствах не сообщайте свой ПИН никому, включая сотрудников Банка и Общества.**

### Меры безопасности при работе в Личном кабинете Страхователя

Для входа в ЛК Вам необходимо ввести Логин (Идентификатор пользователя) и пароль. Для входа в ЛК не требуется вводить никакой другой информации (за исключением случая первоначальной регистрации в ЛК, когда требуется ввести номер действующего Договора).

**Внимание!** Если для входа в ЛК Вам предлагается ввести любую другую персональную информацию или дополнительные данные (номера карт, номер мобильного телефона, Контрольную информацию или другие данные), это указывает на попытку осуществить противоправные действия! В таких случаях необходимо немедленно прекратить сеанс работы в ЛК и срочно обратиться в Контактный центр Общества.

Используйте только надежные и проверенные точки Wi-Fi. Не рекомендуется подключаться к популярным и/или бесплатным точкам доступа Wi-Fi, если Вы не уверены в достоверности имени точки доступа. Обращаем Ваше внимание, что точки доступа Wi-Fi, для подключения к которым не требуется ввод пароля, могут представлять повышенную опасность в связи с возможными действиями мошенников, направленными на получение доступа к Вашим персональным данным.

В случае утери или кражи информации с Логин (Идентификатором пользователя) и паролем Вам следует незамедлительно сменить пароль самостоятельно, либо в случае утраты Логина (Идентификатора пользователя) обратиться в Контактный центр Общества.

При работе с ЛК всегда проверяйте, что установлено защищенное соединение с Официальным сайтом (<https://my.everialife.ru/>) по протоколу https.

В окне браузера должно быть изображение, обозначающее наличие защищенного соединения, которое отличается в зависимости от браузера.

Например, в браузере Microsoft Edge слева от адресной строки располагается серый замочек, при нажатии на который открывается информация о защищенном подключении (см. Рисунок 1).

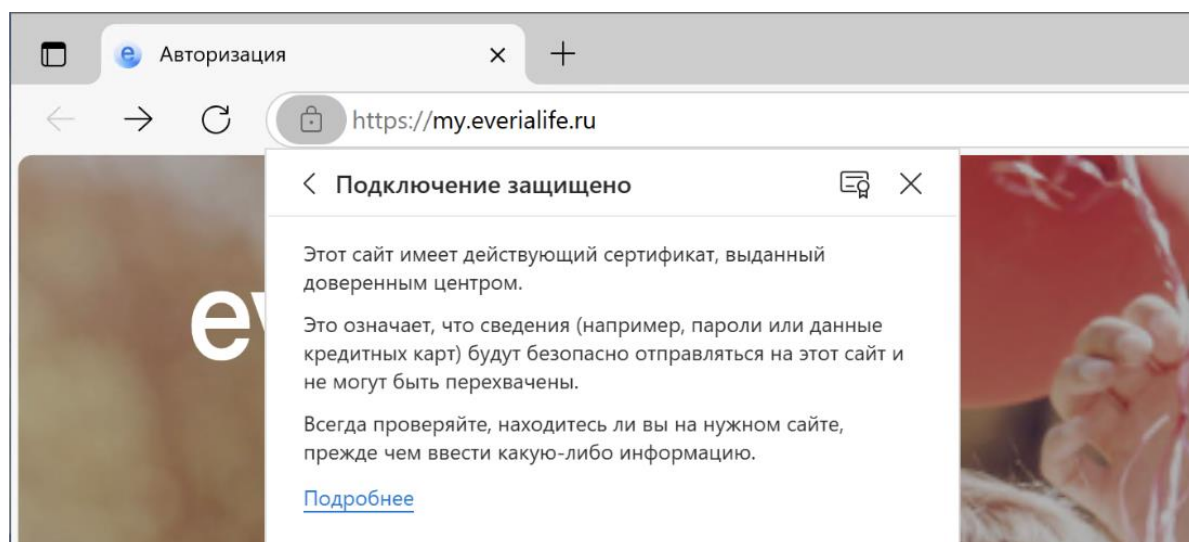


Рисунок 1.

В браузере Google Chrome безопасное соединение можно проверить на иконку слева от адресной строки (см. Рисунок 2).

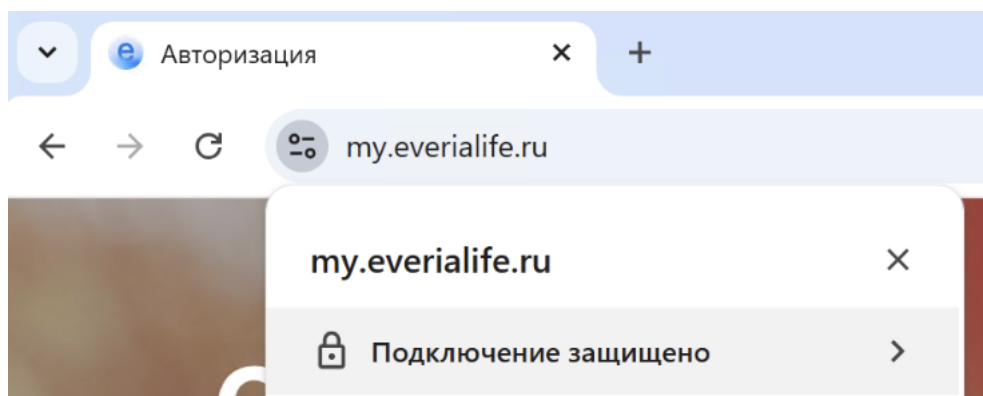


Рисунок 2.

Для проверки того, что Вы подключились именно к сайту Общества можно посмотреть кому выдан сертификат, используемый для безопасного соединения. Для этого нужно нажать на «Подключение защищено» и в открывшемся окне нажать на «Действующий сертификат» (см. Рисунок 3.). В поле «кому выдан» должно быть указано «\*everialife.ru».

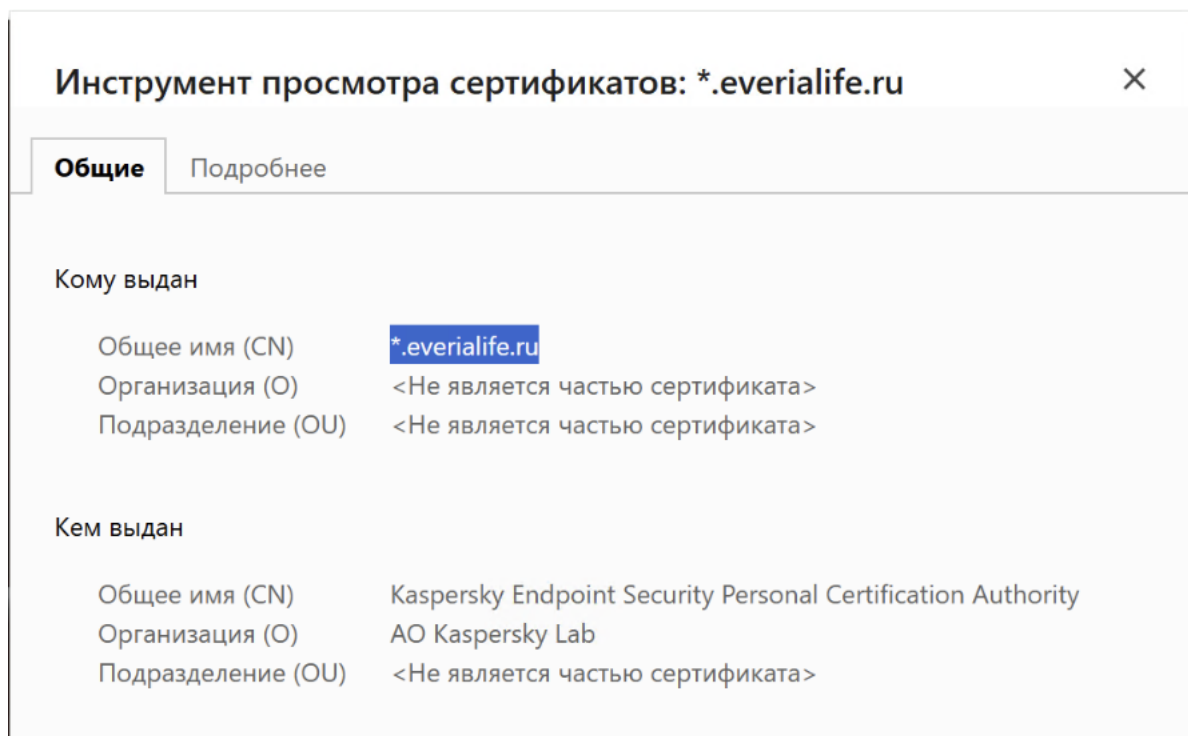


Рисунок 3. Информация о сертификате Общества, используемом для безопасного подключения.

Для мобильных устройств существует специально разработанное Обществом Мобильное приложение. Информацию о приложении можно найти на Официальном сайте Общества.

**Не рекомендуется** использовать ЛК через браузер мобильного устройства, на который приходят SMS-сообщения/Push-уведомления.

Для исключения компрометации Вашей финансовой информации и хищения средств, настоятельно **не рекомендуем** Вам указывать при подключении к услугам Общества номера телефонов или адреса электронной почты, которые Вам не принадлежат.

### Меры безопасности при использовании мобильных устройств

На мобильных устройствах, которые Вы используете для доступа к ЛК и/или для запуска Мобильного приложения:

- используйте современное антивирусное программное обеспечение и следите за его регулярным

обновлением;

- регулярно выполняйте антивирусную проверку для своевременного обнаружения вредоносных программ;
- своевременно устанавливайте обновления операционной системы, рекомендуемые компанией-производителем;
- используйте дополнительное лицензионное программное обеспечение, позволяющее повысить уровень защиты Вашего мобильного устройства – персональные межсетевые экраны, программы поиска шпионских компонент, программы защиты от «СПАМ»-рассылок и пр.

При утрате мобильного устройства необходимо обратиться к оператору связи для блокировки сим-карты. Затем необходимо самостоятельно изменить пароль для доступа в ЛК, а также обратиться в Контактный центр Общества для блокировки доступа в Мобильное приложение.

### **Меры безопасности при работе с Мобильным приложением**

Будьте внимательны – не оставляйте свое мобильное устройство без присмотра, чтобы исключить несанкционированное использование Мобильного приложения.

Устанавливайте бесплатное Мобильное приложение только из официальных онлайн магазинов Google Play, App Store и AppGallery, доступных на Вашем мобильном устройстве или с официального сайта Общества, если такая возможность предусмотрена Обществом. Обязательно убедитесь, что в поле «разработчик мобильного приложения» указано ООО СК «Эверия Лайф».

Помните, что Общество не рассылает своим клиентам ссылки на установку Мобильных приложений через SMS/Push/MMS/e-mail-сообщения.

**Не переходите** по ссылкам для установки Мобильного приложения и не устанавливайте приложения/обновления безопасности, пришедшие в SMS-сообщении, Push-уведомлении или по электронной почте, в том числе от имени Общества.

Установите на мобильном устройстве пароль для доступа к устройству, данная возможность доступна для любых современных моделей мобильных устройств.

### **Защита от SMS/Push-мошенничества**

Мошеннические SMS-сообщения/Push-уведомления, как правило, информируют о блокировке банковской карты, о совершенном переводе средств или содержат другую информацию, побуждающую перезвонить на указанный в SMS-сообщении/Push-уведомлении номер телефона для уточнения информации. Перезвонившему Клиенту мошенники представляются сотрудниками службы безопасности, специалистами службы технической поддержки банка и в убедительной форме предлагают срочно провести действия по разблокировке карты, по отмене перевода и т.п., в зависимости от содержания SMS-сообщения/Push-уведомления. В случае получения подобных SMS-сообщений/Push-уведомлений настоятельно рекомендуем Вам:

- не перезванивать на номер телефона, указанный в SMS-сообщении/Push-уведомлении;
- не предоставлять информацию о реквизитах карты (номере карты, сроке ее действия, ПИНе, CVV2/CVC2/ППК2 коде), Логине (Идентификаторе пользователя) в ЛК, пароле в ЛК, в т.ч. посредством направления ответных SMS-сообщений/Push-уведомлений;
- не проводить через терминалы оплаты никакие операции по инструкциям, полученным на мобильное устройство.

Если полученное SMS-сообщение/Push-уведомление вызывает любые сомнения или опасения, необходимо обратиться в Контактный Центр отправителя SMS-сообщения/Push-уведомления по официальным номерам телефонов, размещенным на официальном сайте отправителя. В случае если Вы все же пострадали от SMS/Push-мошенничества, необходимо:

- немедленно обратиться в Контактный Центр банка, выпустившего карту, по официальным номерам телефонов и заблокировать карту, реквизиты которой были сообщены мошенникам или по которой были совершены незаконные операции;
- немедленно обратиться по телефону к оператору связи, в адрес которого переведены средства, с заявлением о противоправных действиях и возврате средств (как правило, информация о номерах

телефонов, на которые были переведены средства, сотовом операторе и номерах телефонов контактного центра сотового оператора указаны на чеке, полученном в Устройстве самообслуживания);

- немедленно обратиться в Контактный центр Общества по официальным номерам телефонов и сообщить информацию о совершенных незаконных операциях;
- подать через любое подразделение полиции заявление о совершенных противоправных действиях на имя начальника управления «К» МВД России.

### **Защита от e-mail мошенничества**

Мошеннические e-mail-рассылки могут быть использованы злоумышленниками для:

- заманивания получателей сообщений на сайты-«ловушки», на которых под различными предложениями мошенники попытаются получить персональные и конфиденциальные данные (ФИО, Логин (Идентификатор пользователя), Постоянный пароль, Одноразовые пароли, Контрольную информацию, номера банковских карт и их сроки действия, ПИНЫ, CVV2/CVC2/ППК2 коды, Код клиента и пр. информацию). Часто на таких сайтах размещаются вирусы, заражающие компьютеры при открытии страниц;
- принуждения под различными предложениями получателей писем на открытие файла-вложения, содержащего вирус, или переход по ссылке для загрузки вирусного файла.

Признаки того, что e-mail-сообщение является мошенническим:

- в тексте сообщения, как правило, отсутствует или некорректно указана информация относительно Вашего Договора (не указан номер договора страхования, не указаны ваши Имя и Отчество, сумма взноса в случае напоминания об оплате и т.п.);
- сообщения замаскированы под официальные письма Общества и требуют от Вас каких-либо немедленных действий или ответа;

При получении подобного сообщения не рекомендуется переходить по ссылкам, указанным в e-mail сообщении и не открывать присланных вложений.

При возникновении малейших сомнений в подлинности информации, содержащейся в e-mail сообщении, убедительно просим связаться с Контактным центром Общества.

### **Меры безопасности при оплате взносов через платежные терминалы**

**В случае выполнения оплаты в терминале при помощи банковской карты с вводом ПИН-кода ВСЕГДА прикрывайте клавиатуру, например, свободной рукой.** Это не позволит мошенникам увидеть Ваш ПИН или записать его на видеокамеру.

До проведения операции в платежном терминале осмотрите его лицевую часть, в частности, поверхность над ПИН-клавиатурой и устройство для приема карты в Устройстве самообслуживания. В этих местах не должно находиться прикрепленных посторонних предметов или рекламных буклетов. При обнаружении подозрительных устройств, необходимо отказаться от проведения операций в этом терминале.

Не применяйте физическую силу, чтобы вставить карту в платежный терминал. Если карта не вставляется, воздержитесь от использования такого устройства.

**Внимание! Не совершайте на платежных терминалах никаких операций по указаниям посторонних лиц.**