Рекомендации
по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники (далее - вредоносный код), в целях противодействия незаконным финансовым операциям

В соответствии с требованиями Положения Банка России от 17.04.2019 № 684-П «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» ООО «СК «Райффайзен Лайф» (далее также – Компания) обращает внимание своих клиентов, что в случае несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления, возникают следующие риски:

- **совершения злоумышленниками от вашего имени юридически значимых действий и финансовых операций;**
- **получения доступа к вашей конфиденциальной информации и ее разглашения;**
- **воздействия вредоносного кода на ваше устройство, которое используется для выхода в Интернет, работы с сайтом Компании, а также совершения финансовых операций;**
- **нарушения целостности или доступности информации на вашем устройстве;**
- **совершения в отношении вас иных противоправных действий.**

В целях предотвращения возможных негативных последствий вследствие реализации таких рисков рекомендуется принять следующие меры:

- Используйте для работы с сайтом Компании защищенный паролем персональный компьютер или смартфон **с установленным антивирусным программным обеспечением и регулярными обновлениями безопасности операционной системы.** Использование чужого компьютера, как и компьютеров в интернет-кафе, **не является безопасным**.
- Используйте на устройствах исключительно лицензионное программное обеспечение и операционные системы.
- Не устанавливайте стороннее программное обеспечение из непроверенных источников **по просьбе тех, кто представляется сотрудниками банка и иных финансовых организаций**.
- Не устанавливайте и не сохраняйте подозрительные файлы, программы, полученные из ненадежных источников, скаченные с неизвестных сайтов в сети Интернет, присланные с неизвестных адресов электронной почты**. Не открывайте и не используйте сомнительные Интернет - ресурсы на устройстве.**
- Настройте **блокировку экрана** мобильного телефона и скрытие показа содержимого SMS-сообщений на заблокированном экране телефона. Установите пароль (PIN) на SIM-карту.
- Телефоном, на который вы будете получать по СМС одноразовые пароли, **должны пользоваться только вы**. Убедитесь, что доступа к телефону больше ни у кого нет.
- Используйте сложные пароли, состоящие из букв, цифр и специальных символов, которые вы сможете запомнить, **нигде не записывая их.** Не используйте один и тот же пароль в разных информационных системах. Не храните пароли совместно с устройством.
- Никогда и никому не сообщайте ваши аутентификационные данные (**логин, пароль, одноразовые пароли из СМС и т.п.**), в том числе родственникам, коллегам **или тем, кто представляется сотрудниками банка или иной финансовой организации.**
- Помните, что банки **не рассылают** электронных писем, СМС или других **сообщений с просьбой уточнить данные платежей.** Будьте бдительны и не **отвечайте на подобные запросы.**
- Подключите **сервис уведомления об операциях** у своего банка, чтобы контролировать все операции по вашим счетам.
- При входе на сайт Компании **в адресной строке** вашего браузера всегда должен отображаться значок **защищённого SSL-соединения**, а по щелчку на нем — информация о том, что владельцем сертификата является **LLC Insurance Company Raiffeisen Life (raiffeisen-life.ru).**
- При работе с электронной почтой всегда **обращайте внимание на отправителя** сообщения, Компании принадлежат домены **@raiffeisen-life.ru** и **@rlife.me** и только на адреса в этих доменах (например, **info@raiffeisen-life.ru**) сотрудники могут просить отправить почту, и только с них вам может приходить наша корреспонденция. В случае сомнения относительно отправителя сообщения, уточняйте информацию через иные каналы связи, опубликованные на официальном сайте (телефон, обращение в чат, форма обращения на сайте).
- **Перед оплатой премии убедитесь, что маскированные данные** по оплачиваемому договору страхования **соответствуют введенному номеру договора.**

- При переходе на страницу оплаты эквайринга следует проверять наличие SSL соединения и принадлежность сертификата шифрования банку **(online.raiffeisen.ru, АО Raiffeisenbank). Следуйте рекомендациям своего банка при вводе и подтверждении платежных данных.**
- Всегда проверяйте **параметры операции (тип, сумма, получатель)**, содержащиеся в подтверждающем сообщении, **перед вводом кода подтверждения операции**.
- **Незамедлительно проинформируйте Компанию** в случаях совершения или подозрения на совершение третьими лицами мошеннических действий от вашего имени и (или) с использованием вашего устройства, а также его компрометации или подозрения на его компрометацию.