Рекомендации клиенту
по защите информации от воздействия вредоносных кодов
в целях противодействия незаконным финансовым операциям

1. Риски получения несанкционированного доступа к защищаемой информации.

1.1. При использовании системы дистанционного оформления займа и несоблюдении указанных ниже рекомендаций и требований к защите информации, ООО «МКК «Галиция» (далее - Общество) информирует Вас о возникновении рисков получения несанкционированного доступа к защищаемой информации и рисков получения займа лицами, не обладающими правом распоряжения этими денежными средствами.

1.2. Обращаем Ваше внимание на увеличение риска хищения и дальнейшего неправомерного использования ключа электронной цифровой подписи и другой аутентификационной информации при доступе третьих лиц к Вашему мобильному телефону или идентификационному модулю абонента мобильной связи (сим-карте).

2. Возможные риски:

2.1. При утере либо предоставления доступа третьим лицам к мобильному телефону с сим-картой, зарегистрированной на Ваше имя – возможен несанкционированный доступ к просмотру полной информации в Вашем личном кабинете на Сайте Общества: о полученных займах, произведенных платежах, имеющейся задолженности.

2.2. При утере либо предоставлении доступа третьим лицам к мобильному телефону с сим-картой, банковской карте, зарегистрированных на Ваше имя, документа удостоверяющего личность – возможен несанкционированный доступ к Вашему личному кабинету с целью получения займа.

3. Рекомендации по работе в системе дистанционного оформления займа.

3.1. С целью снижения рисков и защиты информации от воздействия вредоносного кода и несанкционированного доступа путем использования ложных ресурсов сети Интернет рекомендуется:

1. Не сообщать посторонним лицам свои персональные данные или информацию о банковской карте через сеть Интернет, логины и коды доступа к ресурсам Общества, историю операций, так как эти данные могут быть перехвачены злоумышленниками и использованы для получения доступа к Вашим счетам, личному кабинету на сайте Общества.
2. Не записывать логин и код на бумаге, мониторе или клавиатуре.
3. Не использовать функцию запоминания логина и пароля в браузерах.
4. Не использовать одинаковые логин и пароль для доступа к различным системам.
5. Не пользоваться системами, требующими ввода логина и пароля, на компьютерах, которые находятся в общедоступных местах и в конфигурации которых Вы не уверены. По возможности совершайте операции только со своего личного средства доступа в целях сохранения конфиденциальности персональных данных.
6. Всегда явным образом завершайте сеанс работы в Личном кабинете на сайте Общества, используя пункт меню «Выход».
7. В случае если операция совершается с использованием чужого компьютера, не сохраняйте на нем персональные данные и другую информацию, а после завершения всех операций убедитесь, что персональные данные и другая информация не сохранились (загрузив в браузере иную web-страницу).
8. Если Вы получили на электронную почту письмо с просьбой обновить или подтвердить персональную и любую другую конфиденциальную информацию со ссылкой на какой-либо сайт (в том числе – сайт Общества), помните, что обновление ключевых персональных данных осуществляется только сотрудником Общества и только по обращению Клиента. Не открывайте ссылки, указанные в сомнительном письме, в котором Вас просят указать конфиденциальные данные. Не звоните по телефонам, указанным в подобных письмах, и не отвечайте на них.

9.9. Соблюдайте условия по конфиденциальному хранению кода, полученному в смс-сообщении от Общества и самостоятельно обеспечивайте условия недоступности кода неуполномоченным лицам.
10. Обеспечивайте надежную и постоянную антивирусную защиту компьютеров, с которых Вы пользуетесь системой дистанционного оформления займа. Обеспечивайте своевременную установку обновлений, выпускаемых разработчиками операционной системы, интернет браузера и антивирусной защиты.
11. Не сообщайте кому-либо, в том числе и сотрудникам Общества, по телефону свой код, полученный в смс-сообщении.
12. В случае, если Вы сообщили сотрудникам Общества свой код, то данная конфиденциальная информация может быть скомпрометирована, Общество может самостоятельно заблокировать вход в Ваш личный кабинет системы дистанционного получения займа.

4. Действия клиента в случае компрометации кода или утери мобильного телефона с сим-картой, банковской карты, зарегистрированных на имя клиента.
4.1. В случае утери кода, мобильного телефона с сим-картой, банковской карты, зарегистрированных на имя Клиента; в случае обнаружения фактов компрометации кода, а также в случае подозрения в компрометации кода Клиент должен незамедлительно сообщить об этом в Общество любым из следующих способов:
По электронной почте info@papazaim.com.
По системе обратной связи на сайте Общества www.papazaim.com.
4.2. Получив от Клиента извещение о компрометации, Общество приостанавливает все операции по выдаче займа и производит блокировку личного кабинета Клиента. Общество пытается связаться по контактным телефонам Клиента, указанным в анкете Клиента.
5. В случае обнаружения несанкционированного списания со счета Общество рекомендует Клиенту осуществить следующие действия: максимально оперативно представить письменное заявление в Общество о факте несанкционированного списания с указанием даты, суммы платежа, других известных Клиенту обстоятельств, а также с просьбой об оказании содействия в возврате несанкционированно списанных денежных средств. Указанное заявление необходимо представить в Общество в срок не позднее 2-х рабочих дней с даты устного обращения в Общество.