РЕКОМЕНДАЦИИ
ДЛЯ КЛИЕНТОВ ООО МКК «ЛИДЕР»
ПО ЗАЩИТЕ ИНФОРМАЦИИ В ЦЕЛЯХ ПРОТИВОДЕЙСТВИЯ НЕЗАКОННЫМ ФИНАНСОВЫМ ОПЕРАЦИЯМ

В соответствии с требованиями Положения Банка России от 17.04.2019 № 684-П[1] ООО МКК «Лидер» (далее - Компания) доводит до вашего сведения основные рекомендации по соблюдению информационной безопасности при использовании официального сайта Компании и отправки обращений (для получения займа необходимо личное присутствие в офисе оформления займов) с сайта Компании.

К защищаемой информации относится следующая информация:

- информация, содержащаяся в документах, составляемых при осуществлении финансовых операций в электронном виде работниками ООО МКК «Лидер»;
- информация, необходимая ООО МКК «Лидер» для идентификации клиентов в целях осуществления финансовых операций и удостоверения права клиентов распоряжаться денежными средствами;
- информации об осуществленных ООО МКК «Лидер» и его клиентами финансовых операциях;
- ключевая информация средств криптографической защиты информации, используемая ООО МКК «Лидер» при осуществлении финансовых операций.

РИСК ПОЛУЧЕНИЯ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ

Реализация риска получения третьими лицами несанкционированного доступа к защищаемой информации может произойти, в частности, в результате доступа третьих лиц к контролю конфигурации устройств, с использованием которых клиентами ООО МКК «Лидер» осуществляется вход на официальный сайт Компании и отправка обращений.

Указанный доступ третьих лиц к контролю конфигурации устройств, с использованием которых клиентами ООО МКК «Лидер» осуществляется вход на официальный сайт Компании и отправка обращений, может быть осуществлен в результате утраты (потери, хищения) такого устройства, утраты клиентом ООО МКК «Лидер» контроля за ним, а также в результате воздействия на него вредоносного кода.

В целях минимизации риска получения третьими лицами несанкционированного доступа к защищаемой информации ООО МКК «Лидер» рекомендует клиентам применять, в том числе, но не ограничиваясь, следующие меры:

1. Обеспечивать безопасность компьютера или иного электронного устройства, с которого осуществляется вход на официальный сайт Компании:

---

[1] «Положение 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 17.04.2019 N 684-П)

- использовать только лицензионное программное обеспечение;
- регулярно обновлять операционные системы и установленное программное обеспечение;
- использовать антивирусное программное обеспечение и регулярно его обновлять;
- ограничить доступ к компьютеру или иному электронному устройству посторонних лиц;
- не работать в системе с компьютера или иного электронного устройства, использующего подключение к общедоступной wi-fi сети.

2. Соблюдать правил безопасного использования информационно-телекоммуникационной сети Интернет:

- ограничить использование сомнительных интернет - ресурсов, сайтов социальных сетей, программ обмена мгновенными сообщениями;
- не устанавливать и не сохранять подозрительные файлы, программы, полученные из ненадежных источников, скачанные с неизвестных интернет - сайтов, присланные по электронной почте с неизвестных адресов;
- не отвечать на подозрительные сообщения, полученные с неизвестных адресов.

3. Использовать пароли:

- использовать надежные пароли, содержащие не менее 8 различных символов (сочетание букв/цифр, большого/малого регистра);
- не допускать передачу паролей, их хранение в открытом виде, в браузерах;
- регулярно обновлять пароли;
- не использовать одинаковые пароли для доступа к различным системам.

При невыполнении или неполном выполнении настоящих рекомендаций по обеспечению информационной безопасности вы принимаете на себя риск получения третьими лицами несанкционированного доступа к защищаемой информации.