Приложение № 1

к приказу от 07.07.2021 № 64-о/д

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

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. Банокм России 17.04.2019 № 684-П) Фонд «Югорская региональная микрокредитная компания» (далее - Фонд ЮМКК) настоящим доводит до сведения своих клиентов информацию о возможных рисках получения несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления.

При осуществлении финансовых операций следует принимать во внимание риски финансовых потерь, связанные с получением несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления, а также с воздействием вредоносных программ. Указанные риски могут быть обусловлены, включая, но не ограничиваясь, следующими ситуациями:

1. Кража идентификатора и пароля доступа или иных конфиденциальных данных посредствам технических средств и/или вредоносного кода и использование злоумышленниками указанных данных с других устройств для несанкционированного доступа.
2. Установка на устройство вредоносной программы, которая позволит злоумышленникам осуществить операции от Вашего имени.
3. Кража или несанкционированный доступ к устройству, с которого Вы пользуетесь сервисами Фонда ЮМКК для получения данных и/или несанкционированного доступа к сервисам с этого устройства.
4. Получение идентификатора доступа, пароля и прочих конфиденциальных данных, в т.ч. паспортных данных, номеров счетов и т.д. путем обмана и/или злоупотребления доверием, когда злоумышленник представляется сотрудником Фонда ЮМКК или техническим специалистом или использует иную легенду и просит Вас сообщить ему эти секретные данные; или направляет поддельные почтовые сообщения или бумажное письмо по почте с просьбой предоставить информацию или совершить действие, которое может привести к компрометации устройства;
5. Перехват сообщений электронной почты и получение несанкционированного доступа к отчетам и прочей финансовой информации, если Ваша почта используется для информационного обмена такой информацией. В случае получения доступа к Вашей электронной почте, отправка сообщений от Вашего имени в Фонд ЮМКК.

К основным причинам возникновения рисков получения несанкционированного доступа к защищаемой информации относятся:

1. Неограниченных доступ третьих лиц к Вашему устройству;
2. Неограниченный доступ третьих лиц к информации о паролях и логинах, используемых для доступа к информационным ресурсам;
3. Несоблюдение режима конфиденциальности в отношении защищаемой информации в информационно-телекоммуникационной сети «Интернет»;
4. Утрата (потеря, хищение) Вашего устройства;
5. Отсутствие проверенного программного обеспечения;
6. Отсутствие действующего актуального антивирусного программного обеспечения с актуальными вирусными базами;
7. Несоблюдение Вами рекомендаций настоящей Памятки.

Все риски, связанные с утратой или компрометацией учетных данных (логин, пароль) и клиентских устройств для доступа к информационным системам Фонда ЮМКК несет Клиент. Фонд ЮМКК не несет ответственность в случаях финансовых потерь, понесенных Клиентами в связи с пренебрежением правилами информационной безопасности.