УТВЕРЖДЕНО
Приказом Генерального директора
ООО МКК «Финансовый супермаркет»
№ 99-22-ФС от «05» декабря 2022 года

_____ / Н.В. Ванин /

РЕКОМЕНДАЦИИ ПО СОБЛЮДЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЦЕЛЯХ ПРОТИВОДЕЙСТВИЯ НЕЗАКОННЫМ ФИНАНСОВЫМ ОПЕРАЦИЯМ

Общество с ограниченной ответственностью Микрокредитная компания «Финансовый супермаркет»

Настоящий документ разработан Обществом с ограниченной ответственностью Микрокредитная компания «Финансовый супермаркет» (далее по тексту – Общество) в соответствии с требованиями Положения Банка России от 20.04.2021 № 757-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» с целью информирования о возможности защиты информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средств вычислительной техники (вредоносный код), в целях противодействия незаконным финансовым операциям.

Рекомендации по соблюдению информационной безопасности (совокупности мер, применение которых направлено на непосредственное обеспечение защиты информации, процессов, ресурсного и организационного обеспечения, необходимого для применения указанных мер защиты) не гарантируют обеспечение конфиденциальности, целостности и доступности информации, но позволяют снизить риски информационной безопасности и минимизировать возможные негативные последствия в случае их реализации.

В целях снижения риска реализации инцидентов информационной безопасности, которые могут привести к риску нарушения выполнения бизнес-процессов, технологических процессов организации и (или) нарушить конфиденциальность, целостность и доступность информации вследствие несанкционированного доступа к Вашей информации лицами, не обладающими правом осуществления значимых (критичных) операций (в т.ч. финансовых), воздействия вредоносного кода на устройства, с которых совершаются критичные (финансовые) операции, совершения в отношении Вас иных противоправных действий, связанных с информационной безопасностью, рекомендуется соблюдать ряд профилактических мероприятий, направленных на повышение уровня информационной безопасности при использовании объектов информатизации (совокупности объектов, ресурсов, средств и систем обработки информации, в т.ч. автоматизированных систем, используемых для обеспечения информатизации бизнес-процессов Общества).

При осуществлении финансовых операций следует принимать во внимание риск получения третьими лицами несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления, такие риски могут быть обусловлены включая, но не ограничиваясь следующими примерами:

- кража пароля и идентификатора доступа или иных конфиденциальных данных, посредством технических средств и/или вредоносного кода и использование злоумышленниками Ваших данных уже на устройствах злоумышленников для несанкционированного доступа;

• установка на устройство вредоносного кода, который позволит злоумышленникам осуществить критичные операции от Вашего имени;

• использования злоумышленником утерянного или украденного Вашего телефона (SIM-карты) для получения СМС-кодов, которые могут применяться Обществом в качестве дополнительной защиты для несанкционированных финансовых операций, что позволит им обойти защиту;

• кража или несанкционированный доступ к Вашему устройству, с которого Вы пользуетесь услугами/сервисами Общества для получения данных и/или несанкционированного доступа к сервисам Общества с этого устройства;

• получение пароля и идентификатора доступа и/или кода из СМС и/или кодового слова и прочих конфиденциальных данных, в т.ч. паспортных данных, номеров счетов и т.д. путем обмана и/или злоупотребления доверием, когда злоумышленник представляется сотрудником Общества или техническим специалистом или использует иную легенду и просит Вас сообщить ему эти секретные данные; или направляет поддельные сообщения по электронной почте или письмо по обычной почте с просьбой предоставить информацию или совершить действие, которое может привести к компрометации устройства;

• перехвата электронных сообщений и получения несанкционированного доступа к выпискам, отчетам и прочей финансовой информации, если Ваша электронная почта используется для информационного обмена с Обществом. Или в случае получения доступа к Вашей электронной почте, отправка сообщений от Вашего имени в Общество.

Для снижения риска Ваших возможных финансовых потерь:

• обеспечьте защиту устройства, с которого Вы пользуетесь услугами Общества, к таким мерам включая, но не ограничиваясь могут быть отнесены:

• используйте только лицензионное программное обеспечение, полученное из доверенных источников;

• не устанавливайте программы из непроверенных источников;

• используйте средства защиты, такие как: антивирус (с регулярно и своевременно обновляемыми базами), персональный межсетевой экран;

• ограничьте доступ к устройству с целью предотвращения несанкционированного доступа;

• устанавливайте своевременные обновления операционной системы, особенно в части обновлений безопасности. Имейте в виду, что обновления снижают риски заражения вредоносным кодом, но не исключают их;

• используйте парольную или иную защиту для доступа к устройству;

• обеспечьте конфиденциальность аутентификационных данных и ключевой информации, полученной от Общества: пароли, СМС-коды, кодовые слова, а в случае вероятной компрометации немедленно примите меры для их смены и/или блокировки;

• не записывайте логин и пароль на бумаге, мониторе, клавиатуре и иных устройствах, с использованием которых осуществляются финансовые операции;

• не используйте функцию запоминания логина и пароля в браузерах для используемых платежных систем;

• не используйте одинаковые логин и пароль для доступа к различным системам;

• регулярно производите смену паролей. Использовать сложносоставные пароли, которые содержат прописные и строчные буквы, а также специальные символы, и не состоят исключительно из имен, номеров телефонов и памятных дат.

Проявляйте осторожность и предусмотрительность:

• будьте осторожны при получении электронных писем с неизвестными ссылками и вложениями, они могут привести к заражению Вашего устройства вредоносным кодом. Вредоносный код, попав к Вам на устройство, через электронную почту или интернет ссылку на сайт, может получить доступ к любым данным и информационным системам на Вашем устройстве;

• внимательно проверяйте адресата, от которого пришло электронное письмо. Входящее электронное письмо может быть от злоумышленника, который маскируется под Общество или ее уполномоченных/доверенных лиц;

• будьте осторожны при просмотре/работе с интернет сайтами, так как вредоносный код может быть загружен с сайта;

• будьте осторожны с файлами из новых или «недоверенных» источников (в т.ч. архивы с паролем, зашифрованные файлы/архивы, т.к. такого рода файлы не могут быть проверены антивирусным ПО в автоматическом режиме);

• не заходите в системы удаленного доступа с недоверенных устройств, которые Вы не контролируете. На таких устройствах может быть вредоносный код, собирающий пароли и идентификаторы доступа или способный подменить операцию;

• при подаче поручений и/или ином обращении в Общество, осуществляйте звонок только по номеру телефона, указанному в договоре или на официальном сайте Общества;

• помните, если Вы передаете Ваш телефон и/или иное устройство другим пользователям, они могу установить на него вредоносный код, а в случае кражи или утери злоумышленники могут воспользоваться им для доступа к сервисам и системам Общества, которыми пользовались Вы. В связи с этим, при утере, краже телефона (SIM-карты), используемого для получения СМС-кодов или доступа к системам и(или) сервисам организации с Мобильного приложения:

1) незамедлительно проинформировать Общество;

2) целесообразно по возможности оперативно с учетом прочих рисков и особенностей использования Вашего телефона заблокировать и перевыпустить SIM-карту, а также сменить пароли и коды доступа (кодовые слова) к сервисам и Обществу;

• при подозрении на несанкционированный доступ и/или компрометацию устройства необходимо сменить пароль, воспользовавшись другим доверенным устройством и/или заблокировать доступ, обратившись в Общество;

• лучше всего использовать для финансовых операций отдельное, максимально защищенное устройство, доступ к которому есть только у Вас;

• контролируйте свой телефон, используемый для получения СМС-кодов. В случае выхода из строя SIM-карты, незамедлительно обращайтесь к сотовому оператору для уточнения причин и восстановления связи.

При работе на компьютере необходимо:

• использовать лицензионное программное обеспечение (операционные системы, офисные пакеты и т.д.);

• своевременно устанавливать актуальные обновления безопасности (операционные системы, офисные пакеты и т.д.);

• использовать антивирусное программное обеспечение, регулярно обновлять антивирусные базы;

• использовать специализированные программы для защиты информации (персональные межсетевые экраны и средства защиты от несанкционированного доступа), средства контроля конфигурации устройств;

• использовать сложные пароли;

• ограничить доступ к компьютеру, исключить (ограничить) возможность дистанционного подключения к компьютеру третьим лицам.

При работе с мобильного устройства необходимо:

• не оставлять свое Мобильное устройство без присмотра, чтобы исключить его несанкционированное использование;

• использовать только официальные Мобильные приложения;

• не переходить по ссылкам и не устанавливать приложения/обновления безопасности, пришедшие в SMS-сообщении, Push-уведомлении или по электронной почте, в том числе от имени Общества;

• установить на Мобильном устройстве пароль для доступа к устройству.

При обмене информацией через сеть Интернет необходимо:

• не открывать письма и вложения к ним, полученные от неизвестных отправителей по электронной почте, не переходить по содержащимся в таких письмах ссылкам;

• не вводить персональную информацию на подозрительных сайтах и других неизвестных вам ресурсах;

• ограничить посещения сайтов сомнительного содержания;

• не сохранять пароли в памяти интернет-браузера, если к компьютеру есть доступ у третьих лиц;

• не нажимать на баннеры и всплывающие окна, возникающие во время работы с сетью Интернет;

• не открывать файлы полученные (скачанные) из неизвестных источников.

Важно помнить и понимать, что безопасность Ваших данных в Ваших руках!