УТВЕРЖДЕНО
Приказом Генерального директора
Общества с ограниченной
ответственностью «Управляющая
компания «ОЛМА-ФИНАНС»
от 14 октября 2019 года № 2019-10-14/1

_____ / К. В. Виноградов /

(подпись) (расшифровка подписи)

Рекомендации
по соблюдению информационной безопасности клиентами ООО «Управляющая компания «ОЛМА-ФИНАНС» в целях противодействия незаконным финансовым операциям

Москва, 2019 г.

1. Общие положения

1.1. 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 «Управляющая компания «ОЛМА-ФИНАНС» (далее по тексту - Организация) доводит до сведения своих клиентов:

- рекомендации по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средств вычислительной техники (вредоносный код), в целях противодействия незаконным финансовым операциям;
- рекомендации о возможных рисках получения несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления;
- меры по предотвращению несанкционированного доступа к защищаемой информации.

1.2. Задачи защиты информации сводятся к минимизации ущерба и предотвращению воздействий со стороны злоумышленников. Для обеспечения надлежащей степени защищенности должен быть обеспечен комплексный подход, когда вопросам информационной безопасности уделяется достаточно внимания, как на стороне Организации, так и на стороне клиента.

1.3. Настоящие рекомендации не гарантируют обеспечение безопасности защищаемой информации, но позволяют в целом снизить риски и минимизировать возможные негативные последствия в случае их реализации.

2. Возможные риски получения несанкционированного доступа к защищаемой информации

2.1. Организация уведомляет своих клиентов о возможных рисках, связанных с получением 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:

- Несанкционированный доступ со стороны третьих лиц к Вашим техническим устройствам (т.е. любому техническому средству, включая, но, не ограничиваясь, компьютер, ноутбук, планшет, мобильный телефон) может повлечь за собой получение третьими лицами доступа к защищаемой информации.
- Кража пароля и идентификатора доступа или иных конфиденциальных данных, например, CVV\CVC номера карты, ключей электронной подписи/шифрования посредством технических средств и/или вредоносного кода; и использование злоумышленниками указанных данных с других устройств для несанкционированного доступа.
- Установка на техническое устройство вредоносного кода, который позволит злоумышленникам осуществить финансовые операции от Вашего имени.
- Использования злоумышленником утерянного или украденного телефона (SIM карты) для получения СМС кодов, которые могут применяться Организацией в качестве дополнительной защиты для несанкционированных финансовых операций, что позволит им обойти защиту.
- 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 Организации 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 Организацией. Или в случае получения доступа к вашей электронной почте, отправка сообщений от Вашего имени в Организацию.

2.2. Несанкционированный доступ со стороны третьих лиц к защищаемой информации может повлечь за собой риски разглашения конфиденциальной информации: персональных данных клиента, сведений об операциях, другой значимой информации.

2.3. Несанкционированный доступ со стороны третьих лиц к защищаемой информации может повлечь совершение такими третьими лицами юридически значимых действий, включая, но, не ограничиваясь, совершение финансовых операций от имени клиента, изменений регистрационных данных клиента, и иных действий, совершенных без воли клиента, и направленных против его интересов.

3. Меры по предотвращению несанкционированного доступа к защищаемой информации и рекомендации по защите информации от воздействия вредоносного кода

3.1. Организация уведомляет своих клиентов о мерах, позволяющих снизить риски несанкционированного доступа к защищаемой информации, снизить риск финансовых потерь включая, но не ограничиваясь:

- Рекомендуется уделять особое внимание к работе с паролями и иной аутентификационной информацией, в том числе:
  - использовать сложные пароли, длинной не менее 8 символов, состоящие из сочетания строчных и прописных букв, цифр и символов, воздерживаться от использования логинов и паролей, установленных ранее при работе с любыми иными ресурсами, сайтами, социальными сетями;
  - регулярно менять пароли на всех устройствах и программах, включая сетевое оборудование;
  - хранить пароль втайне от всех лиц, без исключения;
  - рекомендуется не пересылать пароли по почте, СМС, иным сообщениям или иным образом, не хранить в открытом виде в компьютерных файлах;
  - в случае подозрений на возможную компрометацию (раскрытие) паролей, рекомендуется незамедлительно заменить пароли.
- Рекомендуется организовать надлежащий контроль использования устройства, посредством которого осуществляются финансовые операции, в том числе:
  - исключить или затруднить доступ к устройству третьих лиц;
  - не использовать устройства, используемые для финансовых операций, для работы с сомнительными и развлекательными сайтами (игровые сайты, сайты знакомств, сайты распространения программного обеспечения, музыку, фильмы, социальные и файлообменные сети и т.п.);
  - отказаться или с осторожностью использовать на устройстве для осуществления финансовых операций сетевых пейджеров и сервисов обмена сообщениями (чата, конференций), программ, предназначенных для получения удаленного управления (помощи) данным устройством;
  - обеспечить надлежащее хранение, использование устройства во избежание рисков кражи и/или утери;

- настроить права доступа к устройству с целью предотвращения несанкционированного доступа.

- Рекомендуется не открывать вложения, полученные в электронных письмах от неизвестных отправителей или в случае сомнений в их подлинности.
- Рекомендуется не работать через открытые публичные и не проверенные сети WIFI (кафе, отели, парки, вокзалы и аэропорты).

3.2. Организация рекомендует применять следующие меры по защите информации, от воздействия вредоносного кода включая, но не ограничиваясь:

- Пользуйтесь техническими устройствами с установленным лицензионным программным обеспечением.
- При работе с электронной почтой не открывайте письма и вложения к ним, полученные от неизвестных отправителей, не переходите по содержащимся в таких письмах ссылкам.
- Своевременно обновляйте установленное программное обеспечение и операционную систему (установка критичных обновлений).
- Установите и своевременно обновляйте на техническом устройстве лицензионное антивирусное программное обеспечение с функцией автоматического обновления вирусных баз.
- Осуществляйте проверку жесткого диска персонального компьютера на предмет наличия вирусов и вредоносного программного кода.
- Рекомендуется подвергать предварительному антивирусному контролю любую информацию, получаемую и передаваемую по телекоммуникационным каналам, а также информацию на съемных носителях (магнитных, CD/DVD дисках, USB-накопителях и т. п.). При наличии технической возможности сканирование внешних носителей информации должно осуществляться в автоматическом режиме.
- При работе в Интернет используйте межсетевые экраны. Не устанавливайте каких-либо программ с сайтов, которые вы посещаете.
- Исключите возможность бесконтрольного доступа посторонних лиц (гостей, посетителей) к вашим компьютерам.
- Рекомендуется установить по умолчанию максимальный уровень политик безопасности, не требующий действий пользователя при обнаружении вирусов, лечение (удаление) зараженных файлов должно производиться антивирусным средством в автоматическом режиме.
- При возникновении подозрения на наличие компьютерного вируса (признаки - нетипичная работа устройства, пропадание / появление файлов, частое появление сообщений о системных ошибках и сбоях, значимое замедление работы, увеличение исходящего/входящего трафика и т.п.) рекомендуется провести дополнительные проверки и приостановить работу с финансовой информацией до устранения проблем.
- Следите за информацией в прессе и на сайте Организации о последних критичных уязвимостях и о вредоносном коде.
- Помните, что наличие «эталонной» резервной копии может облегчить и ускорить восстановление вашего технического устройства.