Рекомендации по соблюдению информационной безопасности клиентами АО «УК Мономах» в целях противодействия незаконным финансовым операциям.

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» Акционерное общество «Управляющая компания Мономах» (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 и информирует:

- о возможных рисках получения несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления;
- о мерах по предотвращению несанкционированного доступа к защищаемой информации.

Рекомендации по соблюдению информационной безопасности не гарантируют обеспечение безопасности защищаемой информации, но позволяют в целом снизить риски и минимизировать возможные негативные последствия в случае их реализации.

Организация информирует 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 от 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.

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.

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.

Организация информирует своих клиентов о мерах, позволяющих снизить риски несанкционированного доступа к защищаемой информации, в том числе при утрате (потере, хищении) клиентом устройства, с использованием которого им совершались действия в целях осуществления финансовой операции, контролю конфигурации устройства, с использованием которого клиентом совершаются действия в целях осуществления финансовой операции, и своевременному обнаружению воздействия вредоносного кода, включая, но не ограничиваясь:

Обеспечьте надлежащий контроль использования и защиту устройства, посредством которого осуществляются финансовые операции, в том числе:

- исключите или ограничьте доступ к устройству третьих лиц, в том числе возможность дистанционного подключения;

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

- установите запрет на установку программ из непроверенных источников;

- обеспечьте наличие средства защиты, таких как: антивирус (с регулярно и своевременно обновляемыми базами), межсетевой экран;

- не используйте устройства, используемые для осуществления финансовых операций, для работы с сомнительными и развлекательными сайтами;

- не работайте через открытые публичные и не проверенные сети WI-FI (кафе, отели, аэропорты, вокзалы и т.д.);

- не открывайте вложения, полученные в электронных письмах от неизвестных отправителей;

- обеспечьте надлежащее хранение, использование устройства во избежание рисков кражи и/или утери;

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

Уделяйте особое внимание к работе с паролями и иной аутентификационной/ идентификационной информацией, в том числе:

- используйте сложные пароли, длиной не менее 8 символов, состоящие из сочетания строчных и прописных букв, цифр и символов, воздержитесь от использования логинов и паролей, установленных ранее при работе с любыми иными ресурсами, сайтами, социальными сетями;

- регулярно меняйте пароли на всех устройствах и программах, включая сетевое оборудование;

- рекомендуется не пересылать пароли по почте, СМС, иным сообщениям или иным образом, не хранить в открытом виде в компьютерных файлах;

- храните в тайне аутентификационные/идентификационные данные и ключевую информацию, полученные от Организации: пароли, СМС коды, кодовые слова, ключи электронной подписи/шифрования, а в случае компрометации немедленно примите меры для смены и/или блокировки;

- соблюдайте принцип разумного раскрытия информации о номерах счетов, о Ваших паспортных данных, о номерах кредитных и дебетовых карт, о CVC\CVV кодах, в случае если у вас запрашивают указанную информацию, в привязке к сервисам Организации по возможности оцените ситуацию и уточните полномочия и процедуру через независимый канал, например, через телефон контакт центра Организации;

- не вводите персональную информацию на подозрительных сайтах и других неизвестных Вам ресурсах;

- внимательно проверяйте адресата, от которого пришло электронное письмо. Входящее электронное письмо может быть от злоумышленника, который маскируется под представителей Организации или иных доверенных лиц,

При работе с ключами электронной подписи необходимо:

- использовать для хранения ключей электронной подписи внешние носители, настоятельно рекомендуется использовать специальные защищенные носители ключевой информации (ключевые носители), например: e-token, смарт-карта и т.п.;

- крайне внимательно относиться к ключевому носителю, не оставлять его без присмотра и не передавать третьим лицам, извлекать носители из компьютера, если они (ключевые носители) не используются для работы.

Организация рекомендует применять следующие меры по защите информации, от воздействия вредоносного кода, приводящего к нарушению штатного функционирования средств вычислительной техники, в целях противодействия незаконным финансовым операциям, включая, но не ограничиваясь:

- используйте технические устройства с установленным лицензионным программным обеспечением;

- своевременно обновляйте операционную систему, особенно в части обновлений безопасности, это позволит снизить риски заражения вредоносным кодом;

- 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;

- при работе с электронной почтой не открывайте письма и вложения к ним, полученные от неизвестных отправителей, не переходите по содержащимся в таких письмах ссылкам, они могут привести к заражению Вашего устройства вредоносным кодом;

- 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;

- не заходите в системы удаленного доступа с недостоверных устройств, которые Вы не контролируете, на таких устройствах может быть вредоносный код, собирающий пароли и идентификаторы доступа или способный подменить операцию;

- при работе в Интернет используйте сетевые 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 резервной копии может облегчить и ускорить восстановление вашего технического устройства.