**Уведомление клиентов о возможных рисках информационной безопасности, связанных с несанкционированным доступом, вредоносными кодами и иными противоправными действиями лиц, не имеющим право совершать операции от лица клиента. Рекомендации клиентам по защите от противоправного доступа и о рисках вредоносных программ**

**I. Уведомление о рисках информационной безопасности, связанных с несанкционированным доступом, вредоносными кодами и иными противоправными действиями лиц**

В соответствии с требованиями к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций Акционерное общество «РЕГИОН Эссет Менеджмент» (далее – «Общество») настоящим уведомляет клиентов Общества о возможных рисках финансовых потерь из-за:

∙ несанкционированного доступа к Вашей информации лицами, не обладающими правом осуществления финансовых операций;

∙ потери (хищения) носителей ключей электронной подписи, с использованием которых, осуществляются финансовые операции;

∙ утраты (потере, хищении) устройства, с использованием которого совершаются действия в целях осуществления финансовой операции;

∙ воздействия вредоносного кода на устройства, с которых совершаются финансовые операции;

∙ совершения в  отношении Вас иных противоправных действий.

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:

a. Кража пароля и идентификатора доступа или иных конфиденциальных данных, например, закрытого ключа посредством технических средств и/или вредоносного кода и использование злоумышленниками указанных данных с других устройств для несанкционированного доступа.

b. Установка на устройство вредоносного кода, который позволит злоумышленникам осуществить операции от Вашего имени.

c. Использования злоумышленником утерянного или украденного телефона для получения СМС кодов, которые могут применяться Обществом в качестве дополнительной защиты для несанкционированных финансовых операций, что позволит им обойти защиту.

d. Кража или несанкционированный доступ к устройству, с которого Вы пользуетесь услугами/сервисами Общества для получения данных и/или несанкционированного доступа к сервисам с этого устройства.

e. 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 почтовые сообщения или письмо по обычной почте с просьбой предоставить информацию или совершить действие, которое может привес к компрометации устройства;

f. Перехвата почтовых сообщений и получения несанкционированного доступа к финансовой информации, если Ваша почта используется для информационного обмена с Обществом. В случае получения доступа к вашей почте, отправка сообщений от Вашего имени в Общество.

**Все риски, связанные с утратой и компрометацией учётных данных несет Владелец учётных данных.**

**Общество не несет ответственность в случаях финансовых потерь, понесенных клиентами в связи с пренебрежением правилами информационной безопасности.**

**II. Меры по предотвращению несанкционированного доступа к защищаемой информации.**

1. Обеспечьте защиту устройства, с которого вы пользуетесь услугами Общества, к таким мерам включая, но не ограничиваясь могут быть отнесены:

· Использование только лицензированного программного обеспечения, полученного из доверенных источников.

· Запрет на установку программ из непроверенных источников.

· Наличие средства защиты, таких как: антивирус (с регулярно и своевременно обновляемыми базами), персональный межсетевой экран, защита накопителя.

· Настройка прав доступа к устройству с целью предотвращения несанкционированного доступа.

· Хранение, использование устройства с целью избежать рисков кражи и/или утери.

· Активация парольной или иной защиты для доступа к устройству.

· В случае обнаружения злонамеренного программного обеспечения на компьютере после его удаления незамедлительно смените логин и пароль.

· Не передавайте свою личную информацию через общедоступные Wi-Fi сети. Работая в них, желательно не вводить пароли доступа, логины.

2. Обеспечьте конфиденциальность:

· Храните в тайне аутентификационные/идентификационные данные и ключевую информацию, полученные от Общества: пароли, СМС коды, кодовые слова, закрытые ключи, сертификаты, 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 кодах, в случае если у вас запрашивают указанную информацию, в привязке к сервисам Общества по возможности оцените ситуацию и уточните полномочия и процедуру через независимый канал, например, через телефон Общества.

3. Проявляйте осторожность и предусмотрительность:

· Будьте осторожны при получении писем со ссылками и вложениями, они могут привести к заражению вашего устройства вредоносным кодом. Вредоносный код, попав к Вам через почту или интернет ссылку на сайт, может получить доступ к любым данным и информационным системам на вашем устройстве.

· Внимательно проверяйте адресата, от которого пришло письмо. Входящее письмо может быть от злоумышленника, который маскируется под Общество или иных доверенных лиц.

· Будьте осторожны при просмотре/работе с интернет сайтами, так как вредоносный код может быть загружен с сайта.

· Будьте осторожны с файлами в архиве с паролем, так как в таком файле может быть вредоносный код.

· 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.

· Анализируйте информацию в прессе и на сайте Общества о последних критичных уязвимостях и о вредоносном коде.

· В рамках взаимодействия с Обществом осуществляйте звонок только по официальному номеру телефона Общества, указанному в договоре и / или официальном сайте в сети «Интернет». Важно учесть, что от лица Общества не могут поступать звонки или сообщения, в которых от Вас требуют передать СМС-код, пароль, номер карты, кодовое слово и т.д.

· Имейте в виду, что если Вы передаете ваш телефон и/или устройство другим пользователям, они могу установить на него вредоносный код, а в случае кражи или утери злоумышленники могут воспользоваться им для доступа к системам Общества, которыми пользовались Вы.

· При утере, краже телефона, используемого для получения СМС кодов или доступа к системам Общества необходимо:

a. незамедлительно проинформировать Общество, используя способы указанные в договоре с Обществом;

b. целесообразно по возможности оперативно с учетом прочих рисков и особенностей использования вашего телефона заблокировать и перевыпустить сим карту;

c. сменить пароль, воспользовавшись другим доверенным устройством и/или заблокировать доступ, обратившись в Общество;

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

· отозвать скомпрометированный закрытый ключ, в соответствии с правилами, отраженными в договорных и/или процедурных документах;

· 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 сим карты, незамедлительно обращайтесь к сотовому оператору для уточнения причин и восстановления связи.

· Регулярно выполняйте резервное копирование важной информации.

· Поддерживайте контактную информацию в актуальном состоянии для того, чтобы в случае необходимости с Вами можно было оперативно связаться.

4. При работе с ключами электронной подписи необходимо:

· Использовать для хранения секретных ключей электронной подписи внешние носители.

· Крайне внимательно относиться к ключевому носителю, не оставлять его без присмотра и не передавать третьим лицам, извлекать носители из компьютера, если они не используются для работы.

· Использовать сложные пароли для входа на устройство и для доступа к ключам электронной подписи, не хранить пароли в текстовых документах на компьютере.

5. При работе на компьютере необходимо:

· Использовать лицензионное программное обеспечение (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.

6. При работе с мобильным устройством необходимо:

· Не оставлять свое Мобильное устройство без присмотра, чтобы исключить 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.

7. 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 третьих лиц;

· Не нажимать на баннеры и всплывающие окна, возникающие во время работы с сетью Интернет;

· Открывать файлы только известных Вам расширений (docx, png, xlsx и т.д.).