Рекомендации
по защите информации для клиентов АО «УК «ЭКТО Прайм» в целях противодействия незаконным финансовым операциям

В соответствие с требованиями Положения Банка России от 20.04.2021 N 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» АО «УК «ЭКТО Прайм» (далее по тексту – Управляющая компания) доводит до Вашего сведения

- информацию о возможных рисках несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления;

- информацию о мерах по предотвращению 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.

Деятельность АО «УК «ЭКТО Прайм» по управлению инвестиционными фондами, паевыми инвестиционными фондами и негосударственными пенсионными фондами, связанная с использованием электронно-вычислительной техники, несет в себе риск получения третьими лицами несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций от имени клиента финансовой организации (его уполномоченного лица).

К защищаемой информации относится следующая информация:

- информация, содержащаяся в документах, составляемых при осуществлении финансовых операций в электронном виде работниками АО «УК «ЭКТО Прайм» и (или) клиентами АО «УК «ЭКТО Прайм»;
- информация, необходимая АО «УК «ЭКТО Прайм» для авторизации клиентов в целях осуществления финансовых операций и удостоверения права клиентов распоряжаться денежными средствами, ценными бумагами или иным имуществом;
- информация об осуществленных АО «УК «ЭКТО Прайм» и его клиентами финансовых операциях;
- ключевая информация средств криптографической защиты информации, используемая АО «УК «ЭКТО Прайм» и его клиентами при осуществлении финансовых операций.

I. **Уведомление о рисках информационной безопасности, связанных с несанкционированным доступом к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления, и воздействием вредоносных программ.**

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 (в том числе SMS-кодов) или иных конфиденциальных данных посредством 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 Общества для получения данных и/или несанкционированного доступа к сервисам с этого устройства.
4. Получение идентификатора доступа, пароля, SMS-кодов 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 бумажное письмо по почте с просьбой предоставить информацию или совершить действие, которое может привести к компрометации устройства.
5. Перехвата сообщений электронной почты и получения 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 Общество.

Все риски, связанные с утратой и компрометацией учётных данных (логин, пароль) и клиентских устройств для доступа к информационным системам Общества несет Клиент.

Управляющая компания не несет ответственность в случаях финансовых потерь, понесенных Клиентами в связи с пренебрежением правилами информационной безопасности.

II. Рекомендуемые меры по предотвращению несанкционированного доступа к защищаемой информации и защите информации от воздействия вредоносных программ.

1. Обеспечьте защиту устройства, с которого вы пользуетесь сервисами Управляющей компании. К таким мерам включая, но не ограничиваясь могут быть отнесены:
   - Использование только лицензированного программного обеспечения на устройстве, полученного из доверенных источников.
   - Запрет на установку программ из непроверенных источников.
   - Наличие средств защиты, таких как: антивирус (с регулярно и своевременно обновляемыми базами), межсетевой экран (Firewall, брандмауэр – может входить в антивирус), шифрование всех хранимых данных на устройстве.
   - Активация парольной или иной защиты для доступа к устройству с целью предотвращения несанкционированного доступа.
   - Внимательное хранение и использование устройства с целью избежать доступа 3-их лиц и рисков кражи и/или утери.
   - Недопущение доверия устройства в разблокированном виде третьим лицам.
   - Периодический контроль устройства на предмет несанкционированных изменений аппаратной конфигурации.
   - Организация надлежащего контроля за устройствами и их программной и аппаратной конфигурацией, в том числе с использованием специальных программных средств, с помощью которых совершаются действия в целях финансовых операций.
   - Регламентация доступа к устройствам, с использованием которых совершаются действия в целях осуществления финансовых организаций, запрет доступа к таким устройствам посторонних лиц.

- Своевременные обновления операционной системы устройства и приложений с помощью официальных каналов указанных производителем программных продуктов.

В случае обнаружения вредоносных программ на устройстве после их удаления незамедлительно смените логин и пароль.

Не подключайтесь к Интернет через общедоступные недоверенные Wi-Fi сети. Подключаясь к таким сетям, существует риск компрометации вашего устройства и перехвата доступа к финансовым сервисам.

2. Обеспечьте конфиденциальность:

- Храните в тайне аутентификационные/идентификационные данные, полученные от Управляющей компании: идентификатор, пароль доступа, никому не сообщайте коды из SMS, а в случае их компрометации немедленно примите меры для их смены и/или блокировки аккаунта.
- Соблюдайте принцип разумного раскрытия информации о номерах счетов, о ваших паспортных данных, о номерах кредитных и дебетовых карт в случае, если у вас запрашивают указанную информацию, в привязке к сервисам Управляющей компании.

3. Проявляйте бдительность и осторожность:

- Будьте осторожны при получении электронных сообщений со ссылками и вложениями, они могут привести к заражению вашего устройства вредоносной программой. Вредоносная программа, попав на устройство через электронную почту или ссылку на сайт, может получить доступ к любым данным и информационным системам на вашем устройстве.
- Внимательно сверяйте адрес отправителя, от которого направлено электронное письмо с официальным адресом лица. Входящее письмо может быть от злоумышленника, который маскируется под сотрудника Управляющей компании или иных доверенных лиц. Используйте надёжный почтовый сервис, обеспечивающий защиту от подделки электронного адреса отправителя (такой как Gmail, Mail.ru, Яндекс почта и т.д.).
- Будьте осторожны при просмотре/работе с сайтами в сети Интернет, так как вредоносная программа может быть загружена с сайта.
- Будьте осторожны с файлами в архиве с паролем, так как в таком файле может быть вредоносная программа.
- Не заходите в сервисы Управляющей компании с непроверенных устройств, которые вы не контролируете. На таких устройствах может быть вредоносная программа, собирающая пароли и идентификаторы доступа или способная подменить операцию.
- Анализируйте информацию в прессе и иных общедоступных специализированных источниках о последних известных критичных уязвимостях и вредоносных программах.
- Осуществляйте звонок в Управляющую компанию только по номеру телефона, указанному в договоре. Важно учесть, что от лица Управляющей компании не могут поступать звонки или сообщения, в которых от Вас требуют передать ваш СМС-код, пароль, данные вашей банковской карты (номер карты, ФИО держателя, срок действия, CVC-код), кодовое слово и т.д.
- Имейте в виду, что, если Вы передаете ваш телефон и/или устройство другим пользователям, они могу установить на него вредоносную программу, а в случае

кражи или утери злоумышленники могут воспользоваться им для доступа к системам Управляющей компании, которыми пользовались Вы.

При утере, краже телефона, планшета, персонального компьютера, используемого для доступа к системам Управляющей компании необходимо:

1) незамедлительно проинформировать Управляющую компанию по телефону или любым другим удобным способом;
2) целесообразно по возможности оперативно с учетом прочих рисков и особенностей использования вашего телефона заблокировать и перевыпустить сим карту, на телефонный номер которой приходят SMS-коды;
3) сменить пароль, воспользовавшись другим доверенным устройством и/или сбросить/заблокировать доступ, обратившись в Управляющую компанию.

- При подозрении на несанкционированный доступ и/или компрометацию устройства необходимо сменить пароль, воспользовавшись другим доверенным устройством и/или заблокировать доступ, обратившись в Управляющую компанию.
- Регулярно выполняйте резервное копирование важной информации. Помните, что наличие резервной копии может облегчить и ускорить восстановление данных Вашего устройства. Но резервные копии также должны храниться в защищённом и доверенном месте недоступном для злоумышленников;
- Лучше всего использовать для финансовых операций отдельное, максимально защищенное устройство, доступ к которому есть только у Вас.
- Контролируйте свой телефон. В случае выхода из строя сим карты, незамедлительно обращайтесь к сотовому оператору для уточнения причин и восстановления связи.
- Поддерживайте вашу контактную информацию в актуальном состоянии для того, чтобы в случае необходимости с Вами можно было оперативно связаться.
- Использовать надёжные уникальные пароли (с длиной от 10 символов, используя строчные и прописные буквы и цифры) для входа в Личный кабинет, не хранить пароли в текстовых документах на компьютере.

4. При использовании сервисов 3-их лиц в сети Интернет рекомендуется:

- Не открывать письма и файловые вложения в электронных сообщениях, полученных от неизвестных отправителей, не переходить по содержащимся в таких сообщениях ссылкам.
- Не вводить персональную информацию на подозрительных сайтах, неизвестных и непроверенных ресурсах.
- Ограничить посещения сайтов сомнительного содержания.
- Не сохранять пароли в памяти интернет-браузера, если данным устройством также пользуются другие лица.
- Не нажимать на баннеры и всплывающие окна, возникающие во время работы с сайтами в сети Интернет.
- Открывать файлы только известных Вам расширений (.docx, .xlsx, .pdf и т.д.).

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 в целом снизить риски информационной безопасности и минимизировать возможные негативные последствия в случае их реализации.

При подозрении на несанкционированный доступ и/или компрометацию устройства необходимо сменить пароль, воспользовавшись другим доверенным устройством и/или заблокировать доступ, обратившись в Управляющую компанию.